IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BLIX INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. 19-1869-LPS
	)	
APPLE, INC.,	)	
	)	
Defendant.	)	
	)	
	)	

SECOND AMENDED COMPLAINT

Of Counsel:

Daniel J. Melman
Guy Yonay
Sarah Benowich
Shaoul Sussman
PEARL COHEN ZEDEK LATZER BARATZ LLP
Times Square Tower
7 Times Square, 19th Floor
New York, NY 10036
(646) 878-0800

Mark C. Rifkin
Thomas H. Burt
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
270 Madison Avenue, 9th Floor
New York, NY 10016
(212) 545-4600

ASHBY & GEDDES
John G. Day (#2403)
Andrew C. Mayo (#5207)
500 Delaware Avenue, 8th Floor
P.O. Box 1150
Wilmington, DE 19899
(302) 654-1888
jday@ashbygeddes.com
amayo@ashbygeddes.com

Attorneys for Plaintiff

Dated: February 12, 2021

TABLE OF CONTENTS

Page

Plaintiff Blix Inc. ("Blix" or "Plaintiff") hereby demands a jury trial and alleges the following against Defendant Apple Inc. ("Apple" or "Defendant"):

I. INTRODUCTION

1. At its core, this case is about how Apple, a once disruptive and inventive company, has become an immovable roadblock on the path to innovation.

2. Consumers should have access to the best software and on terms that best suit their needs, chosen through the natural selection process of fair competition on the merits. That evolutionary process drives innovation, ensures competitive pricing, improves user privacy and security, and increases demand for cutting-edge technologies. Apple harms that process by using its increasing monopoly control over Mobile operating systems in the United States to continuously and stifle emerging competitive threats and disruptive technology in order to maintain its market power.

3. This is not case about product design or technical integration; rather, it is about Apple's using anticompetitive contractual restrictions to exclude competition and limit the ability of rivals and threatening technology. Blix is asking to eliminate anticompetitive terms and conditions—not to redesign iOS.

4. In this action, the Court is confronted with the task of determining whether Apple should continue to exclude competitive threats and maintain its unchecked monopoly power to the detriment of consumers, businesses, and innovation.

5. Apple is the most dominant provider of smartphones and smartphone operating systems in the United States. With a market capitalization of over $2 trillion, Apple is the most valuable company in the U.S. and one of the most recognized brands in the world. Apple's ubiquitous iPhone is an American status symbol, marketed as a premium product and sold for about $300 more than the average smartphone.

6. Apple commands a massive and unique user base with a high switching costs for users and substantial barriers to entry for rivals.

7. Through its iPhones, Apple runs a tightly integrated digital ecosystem centered on its proprietary mobile operating system, iOS. In addition to Google's Android OS, iOS is one of two major players in the mobile operating system market, though there are important differences between them. Apple's iOS is the only OS allowed on its devices and is not licensed to other manufacturers. Google, by contrast, does allow users to run a third-party OS on its devices, and licenses its Android OS to a variety of manufacturers.

8. iOS holds a 61.47% share of the mobile operating system ("Mobile OS") market, measured by the number of smartphones on which it runs in the U.S.[1] However, this estimate likely understates the true magnitude of Apple's market share. Given the significantly higher prices that Apple charges for the iPhone in comparison to phones that run Android OS, Apple's market share measured by revenue is likely considerably higher than 61.47%.

9. Even Apple's high market share understates its market power over users and developers. Apple's monopoly power relies upon the centrality of its devices and iOS to the user experience. For decades, Apple has used this dynamic to its advantage, entrenching its power over both consumers and developers. For example, Apple has consistently raised prices on new iterations of the iPhone, without any significant number of consumers switching to Android.[2] And most iOS users do not multi-home, meaning that they do not use both an Apple and Android product, but are instead trapped by the stickiness of the Apple ecosystem.

---

[1] *See* "Mobile Operating System Market Share United States Of America," https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/#monthly-200901-202102

[2] *See* "Yup, it costs $999. But you'll pay it." https://money.cnn.com/2017/09/12/technology/gadgets/iphone-x-price/index.html

10. Correspondingly, because developers cannot reach iOS users on any non-iOS device, they have no choice but to multi-home. Given the size and more lucrative nature of the iOS user base, developers have no choice but to distribute their apps through iOS. As a result of this dynamic, Apple can charge supra-competitive fees and impose restrictive terms on developers in exchange for accessing iOS users.

11. Apple understands that to maintain its dominance, it must identify and neutralize any threat to its power or the anticompetitive effects that flow from it. Therefore, any innovative technological development that lowers switching and multi-homing costs for users, decreases dependence on iOS for developers, and reduces barriers to entry for rivals pose a major competitive threat to Apple.

12. Plaintiff Blix Inc. poses exactly that threat. Blix's patented Messaging Bridge is an innovative tool aimed at promoting true privacy online. After verifying a user's private e-mail address, Blix's Messaging Bridge creates randomly generated incognito aliases to facilitate anonymous e-mail communications. Third-party developers can integrate Messaging Bridge into their apps, allowing users to anonymously engage with those developers. Importantly, Messaging Bridge offers interoperability and flexibility for users, as it can be used on any OS, across media types (e.g., apps, Twitter links, websites, etc.), and with any e-mail client.

13. Messaging Bridge is especially useful for the facilitation of Consumer Single Sign-On ("Consumer SSO"), a service that centralizes a single set of user credentials which can be used to authenticate that user's identity for multiple apps or services across platforms. Because anonymity is an integral aspect of its Messaging Bridge technology, Blix could offer a more secure and private Consumer SSO than its competitors. Furthermore, Blix offers a seamless experience for users to easily link Consumer SSOs to their email clients and addresses.

14. Apple appears to have recognized the nascent competitive threat that Messaging Bridge posed to its marker power in mobile phones and operating systems, particularly as a privacy-focused entrant into the Consumer SSO market. Unlike any other competitor, Blix threatens Apple by offering a more secure and more private solution than Apple's solution while at the same time lowering barriers to switching for users and reducing the dependence of developers on iOS and Apple.

15. In the past, when onerous fees and unreasonable restrictions were not enough to stop iOS developers from offering monopoly-threatening products, Apple has escalated its anticompetitive behavior. The integration of stolen technology into its own products is a well-known chapter in Apple's playbook. Apple frequently takes other companies' innovative features, adds those ideas to its own software products without permission, and then either ejects the original third-party app from its operating systems or suppresses it in iOS App Store searches. This behavior has been so pervasive throughout Apple's history that it acquired its own name, "Sherlocking," after a bygone file and web search tool—the functionality of which Apple conveniently plucked from a third-party developer's product, rendering it immediately obsolete.

16. Apple escalated similarly with Blix. In September 2019, Apple introduced 'Sign in with Apple' as its proprietary Consumer SSO,[3] infringing upon Blix's Messaging Bridge patent and offering the copycat 'Hide my email' feature as its own. Essentially, Apple Sherlocked Blix's technology, and then took steps to use that stolen technology to entrench Apple's dominance in iOS and eliminate the threat of competition in the Consumer SSO market. Specifically, in addition to infringing the patent, Apple abused its power, pretextually removing

[3] *See* "Sign In with Apple will come to every iPhone app: How the new privacy login tool works," https://www.cnet.com/how-to/sign-in-with-apple-will-come-to-every-iphone-app-how-the-new-privacy-login-tool-works/

Blix's e-mail client, BlueMail, from its app stores without reasonable explanation. On information and belief, Apple then used this pretextual conduct to further harm competition by throwing sand in Blix's gears, forcing Blix to divert attention from deploying and scaling Messaging Bridge at a critical moment for the Consumer SSO market, while Apple used its behemothian resources to misappropriate Blix's product. Where Blix could have benefitted from a first-mover advantage in the market spurred by its own innovation, Apple was able to capture a significant portion of that value through anticompetitive means.

17. Blix's Messaging Bridge threatens Apple in two important ways, which Apple has taken anticompetitive action to resist. First, Blix poses a threat to Apple's monopoly power in the Mobile OS market. Second, the ease of integration of Blix's Messaging Bridge into Consumer SSOs threatens Apple's offering in this market.

18. Blix's technology allows iOS users to interact with third-party app developers seamlessly and anonymously. Communications funneled through the Messaging Bridge are completely insulated from Apple's surveillance, preventing Apple from monitoring and cross-referencing communications between iOS users and developers. In essence, Blix offers technology that would make it more difficult for Apple to Sherlock rivals.

19. In keeping with its traditional adhesion approach to developer contracts, Apple revised the contractual provisions in its App Store Review Guidelines to mandate that any app which offers any third-party Consumer SSO must also offer 'Sign in with Apple' as an option. The 'Sign in With Apple' requirement is not based on any technological integration of software functionality embedded in iOS. It is a plain and aggressive exclusionary conduct and contractual tie intended to further raise the walls around Apple's user base, defending and entrenching the iOS monopoly. And it creates a lose-lose-lose situation for Blix and the entire mobile OS user

base. If Blix maintains users' ability to offer an email service that provides users with the ability to authenticate and access to popular email services such as Gmail or Outlook it will trigger Apple's exclusionary restriction and tie, rendering Blix's Messaging Bridge duplicative and obsolete. If Blix resists Apple's tie and removes these authentication methods, then it loses one of its core functionalities, that is, seamless, centralized secure, and private communication across e-mail boxes. If a third-party app chooses not to comply with Apple's anticompetitive requirement, then, per Apple's guidelines, Apple will exclude the app from the App Store. Additionally, forcing developers to use 'Sign in with Apple' increases the amount of developer resources that comes at a substantial opportunity cost and will go toward enriching Apple, rather than innovating and creating richer user experiences.

20. Apple has, as it often does, inserted itself as the intermediary between users and developers through 'Sign in with Apple,' which harms both, by increasing already high switching costs and user lock-in even further.

21. Apple simply reserves its power over users for itself. An iOS user who wants to switch would not be able to bypass Apple's control over 'Sign in with Apple' and easily reestablish communications with developers on Android. Instead, that user would have to log-in to each individual app manually and reenter their information, which discourages switching and intensifies Apple's stickiness.

22. In contrast, Blix's Messaging Bridge is a tool of disintermediation. Its platform-agnostic, user-centric model reduces consumer and developer dependence on iOS and could facilitate an increase in switching or multi-homing by making it easy to sign into non-Apple devices and services privately and securely.

23. Consumers also suffer harm from Apple's exclusion of Blix as a new entrant with a new business model in the Consumer SSO market. Consumers' frustration with trading their privacy and personal data for software and online services is at a new high, leading them away from names like Amazon, Facebook, or Google, which they know surveil them, mine their data, and sell it to advertisers. 'Sign in with Apple,' though it does offer an alternative model, provides a distinction without a difference. It is easy for Apple to offer more privacy in comparison to companies like Google, and their for-profit data mining operations.

24. But the level of privacy Apple offers its users pales in comparison with the new wave of privacy-centric offerings. With its competitive technology, Blix is able to offer users more privacy and control than Apple, which is significant benefit to consumers and a significant and direct competitive threat to Apple.

25. Blix offers an innovative third alternative that asks the least of the end user. Blix provide the login service without taking control of the communication, neither taking payment in the form of data for targeted advertising, or in the case of 'Sign in with Apple' for marketing, nor extracting control of the interaction as its price. In an attention- and data-economy, this is the equivalent of a steeply discounted price.

26. Relatedly, Apple's claim that its anticompetitive behavior is justified by its privacy advantages over other Consumer SSOs is pretextual. Apple acts as an overseer of nearly every iOS-based user relationship and abuses that position to undercut rivals and deepen its moat. Additionally, Apple's many "privacy" justifications for its abusive practices instead act as a shield from scrutiny—either from competitors, iOS users, or antitrust regulators. While Apple claims to be an industry leader in protecting user privacy, Blix actually protects user privacy. Apple's exclusionary conduct harms competition to provide users with more private and more

secure technology. In today's digital economy, this is precious and substantial dimension of competition and well within the boundaries of the harms that the antitrust laws are intended to address.

27. Apple's monopoly power in iOS allows it to use 'Sign in with Apple' to hold developers hostage, offering guidelines and agreements with highly unfavorable terms, under threat of removing access to the critical iOS user base.

28. If allowed to, Blix's innovative technology can offer, quite literally, a bridge over the moat Apple insidiously dug around its captive user base. But instead, it is becoming merely the latest of Apple's long line of victims that have suffered extraordinary injury from Apple's anticompetitive conduct. As a result, Blix's ability to succeed in the marketplace for cross-platform messaging solutions is at grave risk. Indeed, this underscores the anticompetitive intent and effect behind Apple's actions, as cross-platform messaging solutions are a threat to Apple's dominance.

29. Like past competitive threats, Apple seeks to neutralize the danger to its monopoly by misappropriating and weaponizing innovative technologies given to Apple for distribution on iOS, which developers generally cannot forgo. And in addition to the specific consumer harm flowing from Apple's inferior 'Sign in with Apple,' the company's conduct harms consumers generally because developers like Blix cannot invest in new software for iOS users if Apple cannot offer fair access to users nor refrain from stealing patented technology.

30. Apple harnesses its omnipotent market power to deepen the moat it dug around its cash cow, the imprisoned iOS user base, from which it extracts supracompetitive profits, as well as maintaining high barriers to entry for competitors that rely on iOS.

31. Apple's exclusionary conduct harms to the competitive process, and the remedies Blix seeks from the Court in this case center on restoring competition to the Mobile OS and Consumer SSO markets. First, Blix seeks to hold Apple accountable for its infringement upon the patent it appropriated in order to create 'Sign in with Apple.' Blix respectfully asks this Court to protect patented inventions, and to compensate for the damages arising from this patent infringement. Second, and equally importantly, Blix seeks to enjoin Apple from engaging in the anticompetitive conduct which has created and sustained its monopoly power in the Mobile OS market, and to prevent Apple from abusing that power to harm consumers and thwart innovative entry into emerging markets.

32. Apple's conduct, if not constrained by this Court, will further deepen the moat that protects it from meaningful competition.

II. NATURE OF THE ACTION

33. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. §§ 1, *et seq*., and for antitrust violations under the Sherman Act, 15 U.S.C. §§ 1 *et seq*.

34. Plaintiff filed this lawsuit to stop Defendant's unlawful infringement of Plaintiff's patented invention, to halt Defendant's unlawful effort to maintain and extend monopolies by illegally blocking competition, and to obtain damages, an injunction, and other relief.

III. THE PARTIES

35. Plaintiff Blix Inc. is a Delaware corporation with its principal place of business at 101 Hudson Street, Jersey City, New Jersey. Blix is the successor by merger to BlueMail Inc. BVI and BlueMail LLC, the entities that first developed BlueMail, and is the exclusive owner of all claims, including antitrust claims, arising from the injuries Apple caused to the BlueMail business.

36. Defendant Apple Inc. is a California corporation headquartered in Cupertino, California. Apple operates retail stores throughout the country, including in this District, where it sells iPhone devices preloaded with iOS software—including software specially configured for the infringing features of the 'Sign In With Apple' service.

IV. JURISDICTION AND VENUE

37. Plaintiff's claims for patent infringement arise under the patent laws of the United States of America, 35 U.S.C. §§ 1 *et. seq*., including 35 U.S.C. § 271. Plaintiff's claims for antitrust violations arise under the Sherman Act, 15 U.S.C. §§ 1 *et seq*., including 15 U.S.C. § 2. This Court has exclusive subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337 and 1338(a).

38. Apple is subject to this Court's personal jurisdiction. Apple has infringed the '284 patent in Delaware by, among other things, engaging in infringing conduct within and directed at or from this District. For example, Apple has purposefully and voluntarily placed its infringing products as described herein into the stream of commerce with the expectation that these infringing products will be used in this District. On information and belief, these infringing products, including devices running iOS such as iPhones and iPads, have been and continue to be used in this District.

39. Apple employs individuals and operates a retail store at 125 Christiana Mall in Newark, Delaware in this District. Upon information and belief, this store sells more infringing iPhones than any other Apple retail location in the country and sells and/or supports the second-highest volume of infringing products out of any Apple retail location in the country.[4]

[4] *See* D.I. 13-2, Exhibit 2 to Amended Complaint

40. Consumers and software developers use the infringing 'Sign In With Apple' service with Apple devices throughout the District. Apple has provided the 'Sign In With Apple' system, including iOS software containing 'Sign In With Apple,' to software developers in this District. Apple is also selling devices running iOS to consumers in this District and pushing software updates to users in this District. As discussed herein, Apple has specifically instructed software developers, as well as end-users of Apple devices, to use the infringing features of 'Sign In With Apple.'

41. On information and belief, 'Sign In With Apple' is already pre-installed on iOS 13 devices being sold in this District and being offered as a software update to existing iPhone and iPad devices in this District. On information and belief, users in this District are already using the infringing service—for example, to sign in and communicate with applications such as Kayak and Instacart. On information and belief, infringing aspects of 'Sign In With Apple' such as the "Hide My Email" option, are available and being used in this District.

42. Apple repeatedly has availed itself of the jurisdiction of this Court by filing complaints for patent infringement in this District (*see, e.g.*, *Apple Inc. v. HTC Corp. et al*, C.A. No. 11-611-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-544-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-167-GMS; *Apple Inc. v. HTC Corp. et al*, C.A. No. 10-166-GMS; *Apple Inc. v. Atico Int'l USA Inc. et al*, C.A. No. 8-283-GMS).

43. This Court also has personal jurisdiction over Apple because, as alleged herein, it has transacted business in this District; directly or indirectly sold or marketed substantial quantities of its products and services in this District; and engaged in anticompetitive conduct that was directed at, and had a direct, substantial, and reasonably foreseeable and intended effect of causing injury to, the business or property of persons and entities residing in, located in, or

doing business in this District. Apple has conducted business in this District, and it has purposefully availed itself of the resources and the benefits of conducting business in this District. These activities, among others, give rise to Blix's antitrust claims.

44. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391 and 1400 because Apple has a regular and established place of business in this District, is subject to personal jurisdiction in this District, regularly conducts business in this District, and has committed and continues to commit acts of direct and indirect patent infringement in this District. Venue is also proper in this judicial district under 28 U.S.C. § 1391 because a substantial portion of the events or omissions giving rise to Blix's claims occurred in this District.

V. FACTUAL BACKGROUND

A. The Rise of the iPhone

45. Apple was incorporated in 1977 and is headquartered in Cupertino, California. Apple was one of the first companies to design and market mass-produced personal computers. Currently, the company "designs, manufactures, and markets smartphones, personal computers, tablets, wearables and accessories. And it also sells a variety of related services."[5]

46. At the Macworld Conference and Expo in January 2007, Apple's late-CEO Steve Jobs introduced the long-awaited iPhone, which was best described at the time as a synthesis of an internet-enabled mobile phone, and the then-widely popular portable music player device, the iPod.[6] The first-generation iPhone was released on June 29, 2007. It combined

[5] *See* "Description for Apple Inc.," https://finbox.com/NASDAQGS:AAPL/explorer/description

[6] *See* "Watch Steve Jobs Unveil the First iPhone 10 Years Ago Today," https://time.com/4628515/steve-jobs-iphone-launch-keynote-2007/

cellular phone hardware found in handheld devices with Apple's own proprietary software dubbed iPhone OS, which was renamed iOS in 2010.[7]

41. The iPhone offered several features, such as a full screen front-facing design that eliminated the need for a physical keypad, which attracted users, and it quickly gained a large market share.

42. By July 2016, fewer than ten years after the iPhone first launched, Apple reported that over one billion devices had been sold worldwide.

43. Before the iPhone, "handsets were viewed largely as cheap, disposable lures, massively subsidized to snare subscribers and lock them into using the carriers' proprietary services."[8] In contrast, as a tech journalist explained, "Apple retained complete control over the design, manufacturing, and marketing of the iPhone," meaning that unlike previous generations of phones, the maker and not the carrier would control the software updates and security patches.[9]

i. Mobile OS and iOS

44. Like laptop and desktop personal computers that predated the iPhone, mobile devices such as smartphones and tablets require an operating system or "OS" that enables multipurpose computing functionality.

45. An OS for mobile devices (a "mobile OS"), just like the traditional OS used to run any computer, is a piece of software that provides basic functionality to users of smartphones, such as button controls, touch commands, motion commands, and the basic "graphical user

---

[7] *See* "iPhone OS 4 renamed iOS 4, launching June 21 with 1500 new features," https://www.engadget.com/2010-06-07-iphone-os-4-renamed-ios-gets-1500-new-features.html

[8] *See* "The Untold Story: How the iPhone Blew Up the Wireless Industry," https://www.wired.com/2008/01/ff-iphone/

[9] *Id.*

interface", which includes "icons" and other visual elements representing actions that the user can take. A mobile OS also facilitates the installation and operation of apps that are compatible with that particular OS.

46. Before the release of the iPhone, handset manufacturers such as Nokia and Motorola sold cell phones based more on fashion and brand rather than technological innovation. The mobile OS market, dominated at the time by Symbian, BlackBerry OS and Windows Mobile, was staid, corporate-led and focused on enterprise needs.

47. When the iPhone was launched in 2007, the then-dominant mobile OS offerings lacked the flexibility to rapidly expand application offerings beyond communication and basic productivity functions. Those mobile OSs never focused on the seamless integration of third-party software applications and their developers, and due to infighting among manufacturers as well as the complexity of developing on their low-memory hardware, they never developed a thriving ecosystem of third-party software applications.

48. In contrast, iPhone OS (renamed iOS in 2010) showed the potential for third-party applications, multitasking and graphics to meet future consumer demands.

49. As a result, fashion phones declined in popularity and new competitors entered the market for smartphones. For instance, Nokia realized the limitations of its mobile OS, Symbian, and attempted to develop a more advanced system, Maemo, without success. Research In Motion's once-dominant Blackberry also failed to adapt. More flexible, multipurpose mobile OS arose instead, notably from Microsoft and Alphabet (then Google). Microsoft's Windows Mobile OS did not succeed due to the barrier to entry of attracting developers, but Google's Android mobile OS became the other major mobile OS.

50. Unlike iOS, Android is not paired with proprietary hardware, but runs on phones, tablets and other devices made by third parties, including some of the world's largest consumer electronics firms like Samsung and LG. However, despite Google's resources and sophistication, Apple's tactics have allowed it to acquire market power in the US, at or over 61.47% of the Mobile OS and climbing, with a disproportionate share of revenues generated from mobile device and core services.[10]

ii. The Rise of Third-Party Developers for iOS

51. During the early stages of development of the iPhone, Apple recognized the unique characteristics of the software that can be deployed in mobile OS, including iOS, but Apple's then-CEO Steve Jobs did not intend to let third-party developers build native apps for iOS, instead directing them to make web applications for Apple's proprietary Safari web browser.[11]

52. However, backlash from developers prompted Apple to reconsider its position, with Jobs announcing in October 2007 that the company would have a software development kit ("SDK") for third-party developers by February 2008. The SDK was ultimately released to developers on March 6, 2008.

53. The iPhone App Store was launched on July 10, 2008 and on July 11, the second-generation iPhone, the iPhone 3G, was released pre-loaded with support for the App Store.[12] Initially, apps could only be free or paid but in 2009, Apple added the ability of third-party

[10] *See* "Mobile Operating System Market Share United States Of America," https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/#monthly-200901-202102

[11] *See* "Steve Jobs Was Originally Dead Set Against Third-Party Apps for the iPhone," https://www.cultofmac.com/125180/steve-jobs-was-originally-dead-set-against-third-party-apps-for-the-iphone/

[12] *See* "iPhone 3G is finally official, starts at $199, available July 11th," https://www.engadget.com/2008-06-09-iphone-3g-is-finally-official.html

developers to include in-app purchases in their apps which instantly became the dominant way for third parties to monetize apps, especially games.

54. The iOS App Store has ushered in a revolution and fundamentally changed the way mobile device users, including iOS device users, interact and use a number of apps in connection with their devices. Apps—software programs designed to run on smartphones and tablets— currently facilitate and magnify the full range of a device's functionality. For example, apps support consumers' shopping, social networking, food ordering and delivery, personal emailing, newspaper subscriptions, video and music streaming, or mobile gaming. The vast majority of these apps are developed by third-party developers, rather than by Apple.

55. The quality and availability of third-party apps was the major reason the iPhone was able to gain its dominant market share in the first place. To make the iPhone appealing, Apple actively sought participation from third-party developers. Apple used the availability of these third-party applications as the basis of its consumer value proposition, boasting "what's great about the iPhone is … there's an app for that."[13] Apple trademarked "there's an app for that" in 2010 to highlight this unique appeal from its third-party app ecosystem.[14]

56. Because of this thriving app ecosystem, smartphones are now a ubiquitous tool for daily life. Many consumers use these apps for conducting business, to view their work calendars, draft work emails, edit documents, and perform other work functions on mobile devices.

---

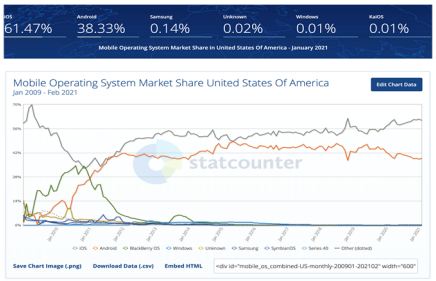
[13] *See* "iPhone 3g Commercial 'There's An App For That' 2009," https://www.youtube.com/watch?v=szrsfeyLzyg

[14] *See* "Apple trademarks 'There's an app for that'," https://www.cnn.com/2010/TECH/mobile/10/12/app.for.that/index.html

57. Currently, the ability to utilize smartphones "on the go" forms part of the distinct value-add of apps to many consumers and businesses. For instance, the portability of smartphones, in conjunction with certain apps, enables uses that could not be replicated by a desktop computer—e.g., real-time GPS-based driving directions, entering meal orders tableside, processing payments at open-air markets and craft fairs, or taking photos and instantly posting them to social media. In short, apps permit the customization of a user's device to cater to the user's specific lifestyle, interests and needs.

iii. Apple's Smartphone Business Model: Selling Smartphones and Smartphone-Related Services

58. Apple possesses significant and durable market power in the market for mobile OS, a highly concentrated market in which only one other firm, Google, has a meaningful consumer base.[15]



59. Apple's iOS has 61.47% of the smartphone operating system market.[16] This market share gives Apple tremendous market power. Further, because smartphone operating system markets have significant network effects that make them prone to market tipping, Apple has only one competitor, Android OS.

[15] *See* "Mobile Operating System Market Share United States Of America," https://gs.statcounter.com/os-market-share/mobile/united-states-of-america/#monthly-200901-202102

[16] *Id.*

60. In 2019 alone, Apple generated more than $142 billion in revenue from the sales of iPhones to customers.[17]

61. Apple installs iOS on all Apple mobile devices and does not license iOS to other mobile device manufacturers. More than 60 percent of all mobile devices in the U.S. run on iOS. Apple is able to commands a premium for these devices: its share of smartphone profits does and has for several years outstripped its market share by unit, and iPhone devices sell at approximately a $300 premium to the other average smartphone.[18] This premium shows signs of price inelasticity: when iPhones have gone up in price, even by hundreds of dollars without corresponding improvements, Apple's U.S. market share has, counterintuitively, only increased.

62. The iPhone is an American status symbol. The "green text bubble" that appears on an iPhone when it receives text messages from other operating systems has become a cultural pejorative[19], and a class signaling mechanism.[20] The iPhone's premium status and unique brand loyalty further feed into its market power.

63. As a result, Apple's control over iOS provides it with gatekeeper power over software distribution and deployment of certain core software functionality on iOS devices.

---

[17] *See* "How Many iPhones Have Been Sold Worldwide? – iPhone Sales Analyzed," https://kommandotech.com/statistics/how-many-iphones-have-been-sold-worldwide/#:~:text=iPhone%20sales%20are%20responsible%20for,35%25%20of%20global%20smartphone%20profits.

[18] *See* "Average price of smartphones in the United States from 2014 to 2024, by segment," https://www.statista.com/statistics/619830/smartphone-average-price-in-the-us/#:~:text=The%20average%20price%20of%20a,580.27%20U.S.%20dollars%20in%202020.

[19] *See* "Sorry, Android users: These iPhone snobs won't date you," https://nypost.com/2019/08/14/sorry-android-users-these-iphone-snobs-wont-date-you/

[20] *See* "Dear iPhone users: Please don't forget that a green bubble is a person.," https://www.androidauthority.com/green-bubble-phenomenon-1021350/;

See "Over 80% of teenagers prefer iPhone to Android — and that's great news for Apple," https://www.businessinsider.com/apple-iphone-popularity-teens-piper-jaffray-2018-4

Apple's gatekeeper power over software distribution and deployment on iOS devices appears to allow it to generate substantial profits from third-party software application developers.

64. The success of iOS has also contributed to the growth and expansion of Apple's Services business segment which now includes the App Store, iCloud, AppleCare, Apple Arcade, Apple Music, Apple TV+, among other services and software features.

65. In 2017, Apple CEO Tim Cook set a goal to rapidly double the size of Services by the end of 2020.[21] Apple met this goal by July 2020, six months ahead of schedule. Services accounted for nearly 18% of total revenue in Fiscal Year 2019, about $46.2 billion. Services grew faster than Apple's hardware sales in recent years, increasing by more than 41% since 2017.[22] Services is also Apple's highest margin business at 63.7% in Fiscal Year 2019 and 67.2% for the quarter ending in June 2020. In 2020, Apple generated $53.7 billion in revenue from Services.[23]

66. Upon information and belief, a significant percentage of Services revenue can be attributed to the company's advertising services which include various third-party licensing arrangements, the App Store platform, and the company's payments services.

67. Industry observers credit Apple's successful focus on growing Services with its rising long-term market valuation. Apple itself has attributed the growth of Services as a driver of the firm's profits from sales and an important factor supporting Apple's overall margins as

---

[21] *See* "Tim Cook: Goal is to double Apple's services revenue by 2020," https://www.cnbc.com/2017/01/31/tim-cook-on-apple-earnings-call-double-services-revenue-by-2020.html

[22] *See* "The Economics of the iPhone," https://www.investopedia.com/articles/investing/022316/economics-iphone-aapl.asp

[23] *See* "Apple made $64 billion from App Store in COVID-19-hit 2020, says report," https://www.businessinsider.in/tech/news/apple-made-64-billion-from-app-store-in-covid-19-hit-2020-says-report/articleshow/80184513.cms

hardware sales slowed or declined. The company has consistently credited app distribution on iOS, licensing sales, and AppleCare for the success of Services.

iv. Apple's Control of App Distribution

70. Since opening its iOS OS to third-party developers the vast majority of apps developed for iOS are developed by third parties. But Apple, which controls iOS, also develops and distributes its own apps.

71. To reach iOS users and make their investment into developing iOS apps viable, app developers need to be able to distribute their apps to iOS users.

72. The iOS App Store allows consumers to easily browse, search for, access reviews on, purchase (if necessary), download, and install mobile apps using just a mobile device and internet connection.

73. Because Mobile OSs have fundamental incompatibilities, developers can distribute only those apps that are compatible with the mobile OS on which the app is run. And iOS device users can only download and use app that are reviewed and approved by Apple.

74. Apple also imposes additional contractual restrictions that foreclose the ability of third-party developers to deploy their software and applications other than through the App Store. In practice, Apple contractual terms prohibit users from downloading apps directly from developers. Apple conditions all app developers' access to iOS on the developers' agreement to distribute their apps solely through the App Store. Section 3.2(g) of the Developer Agreement requires that developers distribute their apps only through the App Store. Apple allows so-called Custom App Distribution, beta distribution through TestFlight, and Ad Hoc distribution for an extremely limited for specific types of commercial use. On information and belief, these channels account for far less than 1% of all apps on iOS.

75. Although Apple states that for "everything else there is always the open Internet," Safari and similar non-Apple Safari-based mobile web applications such as Google's Chrome browser, cannot substitute Apple's App Store because developers cannot deploy essential, core functionalities of their software using the Safari interface.[24]

76. By way of example, standard mail transfer protocol ("SMTP"), a fundamental software functionality and communication protocol for electronic mail transmission, which was first deployed in software in 1982, cannot be deployed – and therefore utilized by iOS users that attempt to access a developer's software – using Safari and similar non-Apple Safari-based mobile web applications. In particular, Safari and similar non-Apple Safari-based mobile web applications do not support IMAP, POP3, SMTP or their equivalents, and Apple has not developed an alternative SMTP that can be utilized by developers that wish to deploy their software through Safari and similar non-Apple Safari-based mobile web applications.

77. Another example is a notification system, a fundamental software functionality that provides a means of delivering a message to a set of recipients and which constitutes an important aspect of modern applications, which cannot be deployed and therefore utilized by iOS users that attempt to access a developer's software using Safari and similar non-Apple Safari-based mobile web applications.

78. Yet another example is the limits on the amount of data that can be transmitted to an iOS user's device by third-party developers. Safari and similar non-Apple Safari-based mobile web applications only allow for the storage of up to 50 megabytes of data, which essentially renders the deployment of most modern software applications impossible.

[24] *See* "App Store Review Guidelines," https://developer.apple.com/app-store/review/guidelines/

79. In addition, unlike iOS applications, Safari and similar non-Apple Safari-based mobile web applications do not offer any storage persistence, an essential feature and functionality of software applications that allows offline access to data that is stored locally on the iOS user's device.

80. Because these key software features and functions cannot be deployed using Safari and similar non-Apple Safari-based mobile web applications, app developers cannot distribute their apps to iOS users through Safari and similar non-Apple Safari-based mobile web applications. Web based apps operating through Safari are typically unable to offer consumers enough features and functionality to reasonably substitute for native iOS apps, and in turn, developers cannot effectively compete with native apps by offering substitutes through Safari, because the technological limits prevent users from substituting web apps for most native apps.

81. In light of the above, Apple's App store is the sole means by which many apps—including apps from Blix—and certain core software functionality and features can be distributed or accessed by iOS consumers.

82. In addition, all software programs, such as apps, must be updated from time to time, either to add functions, to address technical issues, or to ensure compatibility with an OS that has been updated. App updates are important to the continued functionality and commercial viability of apps, as well to make ongoing improvements to each app. Some updates resolve technical or programming issues—e.g., a software fix to a bug that caused the app to crash or to ensure the app remains compatible with an OS update. Other updates are designed to introduce new functionality or content into an app to support continued interest in the app by its users—e.g., an update to a bank app that adds the ability to deposit checks, a business suite that has added new functions for its customers' or employees, or an update to a game that introduces new

challenges or cosmetic features. Thus, in addition to a channel for initial distribution, app developers need a mechanism to inform app users of updates to their apps, and a feasible means of disseminating those updates.

83. Apps are also OS-specific; they must be programmed to function on the particular OS on which they will be downloaded and run. Thus, apps developed for Android OS cannot substitute for apps designed for iOS. Developers who wish to distribute an app to users of devices with different OSs must therefore code different versions of their app for distribution to the different sets of users. To reach iOS device users, developers must program an iOS-compatible version of their app.

B. Apple Maintains its Monopoly Power Through Anticompetitive Conduct

i. Apple's OS market power depends on significant barriers to entry

84. Apple's mobile OS dominance benefits from substantial flywheel effects that protect it from competition. Because Apple is increasingly dependent on Services rather than hardware sales for its revenue, the flywheel effects that protect its mobile OS market power are especially important.

85. Switching from the Apple ecosystem is impeded by a several factors, first of which is cost. The high price tag on smartphone hardware makes switching prohibitively expensive. Apple further entrenches this lock-in by subsidizing its users to upgrade within the iOS ecosystem.[25]

86. Switching is also impeded by the way Apple's technology encourages grouping dynamics. For example, Apple allows family members to access the songs, movies,

[25] *See* "*iPhone Upgrade Program*," https://www.apple.com/shop/iphone/iphone-upgrade-program

TV shows, books, and apps purchased by other family members. Meanwhile apps like FaceTime, Find My, iMessage, and AirDrop work only between Apple device users.[26]

87. Individuals face similar grouping dynamics with their devices. The average American household owns an average of 2.6 Apple devices, and these devices have numerous cross-Apple device sharing functions that only work between Apple devices.[27] Switching one device often degrades this functionality for the new non-Apple device.

88. Further, individual users face personal hurdles to switching even a single device. Switching to a new mobile OS may mean losing access to saved data, because Apple's cloud service does not communicate with other cloud services. It also requires learning an entirely new mobile OS interface, which can be cumbersome during the transition.

89. Developers face similar pressures to develop products for iOS. Because of Apple's large, premium user base, developers must develop for iOS or they forgo the opportunity to reach over one billion high-paying app users. And because Mobile OS users do not Multihome, developers must Multihome to remain in business.[28]

90. Morover, the nature of many apps requires cross communication with the Apple ecosystem. For example, communication apps like email clients, instant messaging and internet-based audio and video call apps, are commercially viable only if both Android and iOS users can use their application. No Android user would download a communication app if they

---

[26] *See* "*Family Sharing. Share your favorite things with your favorite people*," https://www.apple.com/family-sharing/

[27] *See* "America loves its Apple. Poll finds that the average household owns more than two Apple products," https://www.cnbc.com/2017/10/09/the-average-american-household-owns-more-than-two-apple-products.html#:~:text=The%20CNBC%20All%2DAmerica%20Economic,just%20one%20for%20the%20poorest.

[28] *See* Exhibit 1

were not able to use it to communicate with at least 61.47% of their friends, colleagues and family.

91. According to the House of Representatives Subcommittee on Antitrust, Commercial and Administrative Law of The Committee on The Judiciary's "Investigation of Competition in Digital Markets" (the "Judiciary Report"), "Apple has significant and durable market power in the market for mobile OS."[29]

92. The Judiciary Report states that "power over software distribution on iOS devices appears to allow it to generate supranormal profits from the App Store and its Services business."[30]

93. Apple's continued dominance in Services in the coming years depends on maintaining these and other barriers against other entrants. Any threat that makes these and other barriers less effective at locking in users threatens future Services revenue.

ii. Apple's Efforts to Deter, Suppress, and Neutralize Mobile OS Competition

94. The most significant competitive threat to iOS emanates from products that offer users an easy, private, and seamless way to cross Apple's moat, overcome the strong lock-in effect, and join the only other viable alternative, Android or another, yet to emerge, nascent entrant.

95. Apps that promote interoperability between Mobile OS will make it more difficult for Apple to continue to earn supranormal and supracompetitive profits from the App Store and from Services. In particular, technology that promotes interoperability may convince

[29] *See* Exhibit 2

[30] *Id.*

iOS users to 'jump ship,' and join a more developer and user-friendly rival Mobile OS. Alternatively, greater interoperability may give rise to a new, more innovative Mobile OS.

96. Technologies that enable this type of switching make developers less dependent on iOS and thus less willing to pay monopoly rents to Apple. This is a competitive threat to Apple.

97. Apple has used its App Store to restrict functionality or cause arbitrary review challenges for applications that threaten to commodify its hardware and make the iOS operating system nonessential. For example, Apple banned Microsoft's xCloud software in large part because xCloud is a "middleware" that allowed users to access many different games software from the cloud rather than through individual applications written specifically for iOS.[31]

98. Apple's leadership understands that iOS' Mobile OS monopoly is most vulnerable to the emergence of new and disruptive technologies that might be leveraged or utilized to influence consumer behavior or industry standards, and thereby erode the high barriers Apple has erected around its captive user base.

99. Thus, Apple deploys its Developer Agreement to contractually exclude or hamper these technologies. Apple imposes restrictions and makes arbitrary changes to its policies to ensure that innovative technologies that could threaten its power are prevented from growing.

100. Apple does not reserve its anticompetitive behavior to disruptive technologies, however. It has long engaged in a pattern of conduct designed to create and maintain a

[31] *See* "Apple Revises Its xCloud Ban, but Microsoft Isn't Happy," https://www.muo.com/apple-revises-xcloud-ban-microsoft-isnt-happy/

competitive advantage over developers seeking to challenge its dominance and to extract monopoly rents from its dependent developers.

101. Though Apple depends upon third-party developers to supply its customers with a broad array of software to fill an endless array of needs – "There's an App For That" was a foundational Apple marketing slogan for its iPhone devices – Apple also quashes competition with those third-party developers when it sees fit. If an application is a potential threat to any of its products, Apple can banish it from the iOS App Store – the marketplace it controls – by either removing it from the platform going forward entirely or burying it through manipulating search results to make it nearly impossible for users to find.

102. Moreover, because it is functionally impossible for most developers to forgo distribution of their products on iOS, Apple can impose exclusionary restrictions upon developers, over which they have no power to negotiate or decline. These restrictions work to fortify Apple's competitive advantage.

103. As a condition of distributing apps on iOS, Apple requires developers that offer digital products, such as email clients and music streaming apps, to use Apple's in-app payment system for transactions. For most of these apps, Apple takes a 30% cut of app revenue, which, based on information and belief, forces developers to charge higher prices.[32] Importantly, many of the developers subject to this requirement are those which compete directly with Apple's proprietary apps.

[32] *See* "Apple to cut App Store commission to 15% for some devs," https://www.polygon.com/2020/11/18/21573202/apple-small-business-program-app-store-commission; Apple has recently cut the subscription fee for developers generating less than $1,000,000 per year. In addition, Apple reduced its fee from 30% to 15% for certain subscriptions that last more than a year.

104. Apple has been ruthless in its willingness to extract monopoly pricing from dependent developers. In response to accusations that this policy unfairly hurts third-party app developers and leads to fewer apps in iOS, former Apple CEO Steve Jobs said of its commission and in-app payment requirements, "[T]here will be some roadkill because of it. I don't feel guilty."[33]

105. Apple also disadvantages competitors by pre-installing about 40 of its own apps on the iPhone.[34] Because users tend to stick with defaults, Apple's pre-installation tactics serve as a barrier to entry for rivals across app categories.

106. Relatedly, Apple preferences itself in search rankings on the App Store search rankings. Apple's apps show up first in app search results in 60% of basic searches, and 95% of searches related to apps from which Apple derives revenue, such as Apple Music and Apple Books.[35] According to a Wall Street Journal report, Apple Books unseated Audiobooks.com, which had been at the top search result for "audiobooks" for two years, shortly after it was released.[36] This search ranking demotion led to a 25% decrease in audiobook downloads for Audiobooks.com.[37]

---

[33] *See* "Apple conflict with developers escalates ahead of worldwide conference," https://www.bizjournals.com/sanjose/news/2020/06/22/733ae8d4-e516-4418-9998-30414c368c6f.html

[34] *See* Exhibit 2 at 352

[35] *See* "How Apple's Apps Topped Rivals in the App Store it Controls," https://www.nytimes.com/interactive/2019/09/09/technology/apple-app-store-competition.html

[36] *See* "Apple Dominates App Store Search Results, Thwarting Competitors," https://www.wsj.com/articles/apple-dominates-app-store-search-results-thwarting-competitors-11563897221

[37] *Id.*

107. In the past, Apple has justified anticompetitive behavior under the banner of preserving consumer privacy. However, its actions prove that Apple's privacy concerns are merely pretextual.

108. For example, Apple alleges that its in-app-purchase policies that force developers to pay 30% commissions are necessary to ensure user privacy. However, apps that trade physical goods or services, like Uber or Lyft, are not required to use Apple's in-app purchase software. The fact that different categories of apps are treated differently on the same mobile OS makes clear that the motivation cannot be privacy alone.

109. Moreover, despite regular proclamations about its focus on privacy, Apple is being investigated by the House Committee on Energy and Commerce for giving "highly misleading or blatantly false" information in its App Privacy labels product.[38] Competitor apps like WhatsApp allege that Apple's privacy labels are a ploy to disadvantage competitor apps because Apple's own apps would not be restrained by the labels because they are preinstalled.[39] This would give Apple communication products further insulation against competitive pressures from more private applications. While privacy is a commendable goal in the abstract, Apple's privacy efforts have shown to be inadequate and more often, the invocation of privacy is a pretextual justification for more restrictive control over the iOS ecosystem.

[38] *See* Exhibit 3 at 1

[39] *See* "WhatsApp criticizes Apple privacy labels as anti-competitive," https://www.cnet.com/news/whatsapp-reportedly-criticizes-apple-privacy-labels-as-anti-competitive/

iii. Stealing Innovation Using the App Store

110. Apple's pattern of behavior leveraging the innovation of others to amplify its monopoly power is also well documented.[40] As former CEO Steve Jobs once said plainly, "[w]e have always been shameless about stealing great ideas."[41]

111. Apple's Developer Agreement provides that Apple may create apps that "perform the same or similar functions as, or otherwise competes with" third-party apps.[42] It also provides that "Apple will be free to use any information, suggestions or recommendations [developers] provide to Apple pursuant to this agreement for any purpose."[43] Taken together, these two provisions almost explicitly inform developers that Apple can and will use their competitively sensitive information to compete with them. Developers have no choice but to accept these highly unfavorable terms because Apple holds monopoly power over them.

112. Apple's own former director of App Store review, Phillip Shoemaker, has admitted that "Apple gets a lot of inspiration from apps that are on the App Store." Mr. Shoemaker further confirmed that Apple collected and analyzed App Store data on third-party applications to decide what ideas Apple would include in its own offerings. He said, "Top Apple executives" could "peek at apps under review," and that decisions on which new apps to develop were "made at the top rungs of the company." Mr. Shoemaker would then receive "regular

[40] *See* "How Apple Uses Its App Store To Copy The Best Ideas," https://www.washingtonpost.com/technology/2019/09/05/how-apple-uses-its-app-store-copy-best-ideas/

[41] *See* Exhibit 2 at 364

[42] *See* Exhibit 4, "Apple Developer Agreement," Clause 11

[43] *Id*.

emails from angry app developers, irked that the company had rejected their app or, in some cases, killed their app off by copying them."[44]

113. Apple's practice of identifying and then copying the innovations of other software developers is so well known in the industry that it has its own term. "Sherlocking" refers to a web and file search tool, Sherlock, introduced on MacOS approximately 20 years ago, which was apparently created by a third-party developer whose product was made essentially irrelevant by Apple.[45] In this instance, Apple's pattern of anticompetitive conduct stretches back decades, and has helped to ingrain and amplify its monopoly power.

114. Specifically, Apple recognizes that so long as it keeps new and threatening technologies at bay and from operating at scale, it will be harder for new firms to enter and build scale around another Mobile OS. Numerous app developers have been Sherlocked by Apple, submitting to App Review, only for it to be rendered irrelevant by Apple without consequence.

115. Apple's strategy to maintain its monopoly in the Mobile OS market forecloses competition and harms consumers —reducing consumer choice, discouraging third-party software developers from investing in future innovative products, reducing competition among applications, and forcing up anticompetitive prices for digital goods and services sold through the App Store.[46] Apple will continue to pursue its "embrace and extend" strategy unless enjoined from doing so.

---

[44] *See* "How Apple Uses Its App Store To Copy The Best Ideas," https://www.washingtonpost.com/technology/2019/09/05/how-apple-uses-its-app-store-copy-best-ideas/

[45] *See* "Sherlock (software)," https://en.wikipedia.org/wiki/Sherlock_(software)#Sherlocked_as_a_term

[46] *See* Section C(ii)

C. The Relevant Markets and Apple's Monopoly Power

i. Mobile OS in the United States

116. Mobile OS is a relevant product market. Mobile OS consists of system software that manages smartphones, tablets, or other mobile devices' hardware, software resources, and provides common services for mobile applications. Mobile OS is a unique and distinct software product.

117. The relevant geographic market is the United States. The United States is a relevant geographic market for Mobile OS. There are many barriers between countries in the Mobile OS market due to differences in cellular network access, regulatory regimes, and social norms which vary at the country level. In addition, network effects between users are generally stronger between users in the same country because for most users the vast majority of relevant friends, family, and other personal connections reside in the same country as the user. Accordingly, users in the United States predominately interact with other users in the United States. For users in the United States, a Mobile OS that is not popular in the United States, even if it is popular in another country, is therefore not reasonably interchangeable with a Mobile OS that is popular in the United States. Apple and other industry participants recognize these distinctions and track their performance, and that of rivals, separately by country.

118. While users may engage with other OSs, other types of OSs are not adequate substitutes for Mobile OS.

119. Mobile OS is distinct from, and not reasonably interchangeable with, traditional personal computer OS. The dominant operating system for personal computers in the U.S. and the world, Windows, will not run on the vast majority of mobile devices. Providers of Mobile OS are often providers of fully distinct personal computer operating systems. For example, Google offers Chrome OS for personal computers as a separate product from its

Android Mobile OS. Apple does the same, offering macOS for personal computers and iOS for mobile devices. Personal computers differ so much from mobile devices in their size, function and features that they are not used for the same purposes and are treated by businesses and consumers alike as separate products. The price of traditional operating systems does not discipline the prices of mobile OS.

120. Mobile OS is distinct from, and not reasonably interchangeable with, other types of software. Application software depends on an operating system to run and therefore is a complement and not a substitute. Certain kinds of software are sometimes called "middleware" and can mediate (or disintermediate) the relationship between operating systems and applications software, but they too are incapable of actually running the hardware resources and therefore leave the user in need of an operating system for their device. Although it presents a disruptive competitive threat to Apple, middleware is not a substitute for Mobile OS, and prices of middleware do not discipline the price of Mobile OS.

ii. Apple's Monopoly Power in the Mobile OS Market

121. Apple offers iOS, its Mobile OS to users via its proprietary hardware. As the House Digital Markets Report notes, "Apple installs iOS on all Apple mobile devices" and enjoys "significant and durable market power in the market for mobile operating systems." Similarly, Mr. Cook testified in 2020 that the value Apple provides to its users is "its seamless integration of hardware and software."[47]

122. Apple's iOS has been the dominant Mobile OS in the United States since at least 2012.

[47] *See* Exhibit 2 at 334

123. Apple holds monopoly power in the Mobile OS market in the United States and has held such power continuously since at least 2015.

124. Apple has maintained a dominant share of the U.S. Mobile OS market (in excess of 50%) since October 2015, until the present day. This market share averages more than 55% though it often exceeds this, sometimes reaching above 60% as it did in 2020. It is likely to continue to hold monopoly power for the foreseeable future.[48]

125. Apple's dominant position in the U.S. Mobile OS market is durable, due to significant entry barriers, including direct and indirect network effects and high switching costs.

126. Direct network effects include user-to-user effects that make Mobile OS more valuable as more users join the service. Apple offers many exclusive communications applications such as Facetime, which allow users to connect to other iOS users, but offer less or no functionality for connection to Android users. These applications create direct network effects: the more end users on iOS, the greater the value to users on iOS.

127. Indirect network effects are an even greater barrier to entry into Mobile OS. Specifically, a Mobile OS is at the center of an ecosystem with a plethora of participants and an array of stakeholders, such as developers of compatible apps, the makers of ancillary hardware (e.g., headphones or speakers), cellular carriers, and others. Being connected to these providers in the same ecosystem greatly increases the value of the OS to its users, as the more investments that are made by the various stakeholders, the more benefits accrue to the goods and services connected to the network. Apple's iPhone and iPad customers therefore benefit from substantial indirect network effects of being plugged into the iOS ecosystem. A new entrant would need to

[48] *See* Exhibit 2 at 103

launch with an entire ecosystem of hardware and software complements sufficient to immediately attract a large user base.

128. These indirect network effects are also a significant barrier to entry into Mobile OS because they work in the opposite direction: the more the offerings on the ecosystem attract consumers to a Mobile OS, the more essential interaction with that Mobile OS and its user base is for developers.

129. A new entrant to Mobile OS would either need to rapidly acquire a large enough user base to attract an entire ecosystem of developers and other makers of complementary products; or, in the alternative, would have to massively subsidize and coordinate such a supporting set of complementary offerings until such time as the user base grew to support it. Moreover, Apple's gatekeeper power over software distribution on iOS devices allows it to defeat any attempt to distribute such a competitive ecosystem of products to users of its devices.

130. Any potential entrant in Mobile OS market would also have to overcome users' reluctance to incur high switching costs. Over time, users of a given Mobile OS purchase and rely on compatible apps and develop a history of usage and shared experiences, which they would lose by switching to another Mobile OS. Further, these switching costs can increase over time—a form of a "one-way ratchet effect"—as each user's collection of content, purchasing of apps and use of Mobile OS specific services, and investment of effort in building each, continually builds with use of the service.

131. As a result of these and other factors, iOS users seldom switch to Android, and thus developers cannot abandon the Apple OS. This preserves Apple's market power and

contributes to its consistently rising Mobile OS market share over the last decade.[49] This trend is likely to continue in the absence of a proliferation of Middleware and other technologies that lower barriers to switching.

iii. Consumer Single Sign-On in the United States

132. Consumer Single Sign-On Market is a relevant product market. A Consumer Single Sign-On, or "Consumer SSO" is a service that centralized the authentication of identity and credentialing of user permissions for a single user's relationship with many or all the developers and service providers with which the consumer has relationships.

133. Historically, when end users have formed and maintained relationships with online firms that require authentication to access an account, they have done so through a username and password system where the login relationship is unique to that user-firm relationship. That is, an end user traditionally had a username and password with one or more email providers, one or more streaming companies, one or more written media companies, retailers, or other providers. But many end users now have so many of these relationships to maintain, that the proliferation has created a need for new classes of services.

134. One set of these services is a relatively straightforward tool, which is distinct from SSOs. A password manager preserves the existing structure where every relationship has a separate login. Password managers like LastPass simply provide a tool that allows users to keep those logins separate while supplying automated, secure passwords that the user does not have to remember. It is the digital equivalent of keeping all of one's passwords on a physical notepad. Password managers are distinct from Consumer SSO. They are technologically separate, with

[49] *See* Simon O'Dea, "Market Share of Mobile Operating Systems in the United States from January 2012 to December 2019," STATISTA (Feb. 27, 2020), https://www.statista.com/statistics/272700/market-share-held-by-mobile-operating-systems-in-the-us-since-2009/.

different software, historical antecedents, and protocols. They serve different functions and are offered by different providers. They are not a reasonable substitute for a Consumer SSO.

135. The other and more elegant solution is to centralize the relationships themselves. Companies have done this internally, for example providing their employees with a single set of credentials to access different data and applications for work, and in this context the process is called a "single sign-on" or "SSO." Some SSOs work through a protocol called OAuth, and the term is sometimes applied by software professionals in a more colloquial way to refer to SSO. Consumer SSOs are a recent historical development, an SSO not for specialized or organizational purposes, but to allow the ordinary user of social media and applications software to use a single set of credentials to centralize many or all their sign-ons. Consumer SSOs both streamline the sign in process and greatly reduce the security risks inherent in having many passwords and usernames, some of which may overlap, available to a wide variety of service providers.

136. Another benefit of Consumer SSOs, that is also a feature that differentiates them password managers, is that they do not require the user of a given app or service to provide the developers of said app or service with their password credentials . This feature allows users to use less trustworthy services without the risk of a data breach.

137. But this benefit has its limitations. Consumer SSOs do not require the user of a given app or service to provide the developers of said app or service their password credentials, but once the user desires to interact with the app's developer in any other meaningful way, such as subscribing to a newsletter, completing a purchase of goods, or sending feedback, their email address, and by extension, their identity is revealed. Thus, although Consumer SSOs reduce the

risk associated with transacting or using unknown or new services online, they do not eliminate it.

138. Internal corporate SSOs are not offered for consumer purposes, do not allow consumers to manage their relationships with consumer service providers, are not offered to end consumers by the vast majority of consumer developers and are not reasonably substitutable for a Consumer SSO.

139. There are a number of readily familiar Consumer SSO providers in the market: Facebook Login, Google Sign-In, Sign in with Twitter, Sign In with LinkedIn, Login with Amazon.

140. Consumer SSOs are a distinct and separate product from Mobile OS software, and many of the firms that offer Consumer SSOs are companies like Facebook and Amazon that do not compete in the Mobile OS market or offer Mobile OS products. In addition, when given a choice, consumers use popular Consumer SSOs such as Sign In With Facebook both on Android and iOS irrespective of the fact that Google offers its own Consumer SSO. Finally, Facebook and Amazon, companies without market power in Mobile OS, do not bundle their Consumer SSOs to any particular OS and do not condition the usage of their respective Consumer SSO upon the use of a particular OS.

141. These entrants offer login services at what is effectively a non-monetary price. The end user offers up data that Amazon or Facebook or Google (primarily engaged, respectively, in online retailing and in advertising) monetize by mining it to target advertising.

142. There are significant barriers to entry in this market. A new entrant would have to invest in sufficient server capacity to handle enormous throughput with high reliability and invest in security because a Consumer SSO trades a single strong point of failure for many

weak points. Network effects are also a significant barrier to a new entrant. The provider must have a value proposition that is attractive to consumers, which includes being able to use the service to centralize a wide array of service provider relationships. The more of an end user's current or foreseeable service providers there are using a Consumer SSO, the more attractive it will be to end users, while the more end users are on a Consumer SSO, the more attractive it will be to developers.

143. These entrants into this market use their household names and reputation for convenience and as a selling proposition and offer the service free to the end user because they can monetize the data collected through their secure SSOs.

144. Apple's 'Sign In With Apple,'[50] a relativity new entrant to this market, offers a different business model with a distinct value proposition. 'Sign In With Apple' places Apple as the necessary intermediary between a firm seeking to allow its users to access its app or service and the firm's end user. Apple offers this service in conjunction with a disruptive new feature, 'Hide My Email', a private proxy relay that infringes Blix's '284 patent.[51] [52] Apple markets the 'Hide My Email' prominently in its own presentations of 'Sign In With Apple,' and argues that it Consumer SSO is superior in comparison to the offerings of existing market participants due to this privacy oriented feature.[53]

[50] *See* "What is Sign in with Apple?" https://support.apple.com/en-us/HT210318

[51] *See* "Hide My Email for Sign in with Apple," https://support.apple.com/en-us/HT210425

[52] *See* Section E(ii), Section F(ii)

[53] In the WWDC panel introducing "Sign In With Apple", Apple began touting the Hide My Email feature in the first five minutes, at 3:47 of the talk.

145. Apple's foray into the Consumer SSO market is part of a strategic decision the company has made to position itself as a 'leader' in consumer privacy by marketing the future foundation of iOS as being centered on privacy.

146. For example, in the wake of the Cambridge Analytica scandal, Tim Cook capitalized upon the broad outrage by contrasting Apple business model to Facebook's when he said that "we care about the user experience. And we're not going to traffic in your personal life…I think it's an invasion of privacy…privacy is a human right. It's a civil liberty…in something that is unique to America, you know, this like freedom of speech and freedom of the press, and privacy is right up there for us."[54]

147. Upon information and belief, Apple not only desired to compete in Consumer SSO market, but also to protect its iOS monopoly. A cross-platform Consumer SSO that does not compromise or monetize user data greatly reduces switching costs for iOS users and has the potential to deeply erode Apple's moat around those users.

148. Apple uses the pretext of privacy as a false token for the purpose of further locking in users and developers within iOS and further solidifying its monopoly power.

149. The use of 'Sign In With Apple' as an SSO solution then automatically increases user switching costs and widens the moat for users that desire to switch from iOS to Android. Via 'Sign In With Apple', Apple positions itself in a prime position, smack in the middle of the communication chain between the user and the app, and controls this relationship.

150. In particular, users of 'Sign In With Apple' need to reestablish anew all of their communications with the various apps they use in IOS because neither they nor the app

[54] *See* "Apple CEO Tim Cook: 'Privacy to us is a human right...a civil liberty'," https://www.cnbc.com/2018/04/10/apple-ceo-tim-cook-on-the-importance-of-consumer-privacy.html

developers are able to bypass Apple (which exclusively knows how to route communications by hiding the user's public email addresses) and reestablish communications directly or on Android. Instead, users who wish to switch will have to log in manually into each app and add their contact information, a lengthy process that discourages cross-platform migration and makes iOS further sticky and widens the moat.

151. And, notably, the way in which Apple rolled out and promoted 'Sign In With Apple' in iOS, was designed to stifle competition and innovation from privacy-focused SSOs.

152. In particular, Apple's anticompetitive conduct suppressed Blix, a nascent competitor, from scaling a competing Consumer SSO that offers better privacy than 'Sign In With Apple' in a way that defuses of the stickiness of iOS and has the potential to reduce barriers to switching and for consumers and developers t by implementing a seamless, private, and secure cross-platform Consumer SSO solution.

153. Apple's entrance into the Consumer SSO market is analogous to the behavior that Microsoft engaged in during the late 1990s. Back then, Microsoft engaged in exclusionary behavior that inhibited the adoption of middleware technologies that reduced barriers to entry and made it easier for users to switch or multihome with other OSs and allowed developers to reduce dependence on Windows. In this present case, Apple decided to launch its own proprietary Consumer SSO in order to inhibit the adoption of the next generation of Consumer SSO technologies that can reduce barriers and make it easier for users to switch or multihome with other Mobile OSs and will allow app developers to be less dependent on Apple.[55]

154. Apple has been able to gain a significant foothold in the Consumer SSO market by engaging in two distinct types of anticompetitive activities. First, it engaged in exclusionary

[55] *See* Section D(iv)

conduct against its closest competitive alternative, Blix. Second, it used its gatekeeping power over distribution in iOS and its monopoly power in the Mobile OS market to force the adoption of 'Sign In With Apple,' by implementing a contractual tie in the App Store Developer Guidelines. And most app developers are now subject, if they want to offer their apps in iOS, to a requirement that they offer a feature that would allow Apple, down the road, to take away their access to all Apple iOS users. They are subject to the requirement even if they are already doing business with a different provider of Consumer SSO.

155. conduct, on information and belief, a substantial and growing amount of app developers that consume Consumer SSOs have been forced integrate Apple's Consumer SSO, 'Sign In With Apple,' into their apps.

156. Finally, Blix is harmed by Apple's ongoing contractual tie which forces Consumer SSO consumers, namely app developers, to consume Apple's product.

D. A New Threat to Apple's Mobile OS Monopoly Emerges

i. Blix's '284 Patent

157. Plaintiff's BlueMail email service and the Blix Messaging Bridge position Blix as one of the world's most innovative communications companies. Blix's BlueMail repeatedly has won awards for its trailblazing features and its first-in-class user experience.

158. In 2013, Blix began conceptualizing software features that are based on the '284 patent, entitled "Systems and Methods of Controlled Reciprocating Communication[.]," which was first filed on May 13, 2013 and duly and legally issued on August 29, 2017 by the United States Patent and Trademark Office. Blix is the owner by assignment of the '284 patent.[56]

[56] *See* Exhibit 5.

159. The application for the ’284 patent was first published on April 21, 2016, more than a year before the patent was duly and legally issued.

160. The claims of the ‘284 patent describe an innovative improvement to the operation of communications networks, and specifically, to the ability to manage interactions on communications networks, including a specific architecture to manage interactions employing both private and public interaction addresses.

161. The ‘284 patent recites a number of implementation details that offer an innovative solution to the problems of privacy and security in modern communications networks. These implementation details include the use of specific private and public interaction addresses in a communications network.

162. At the heart of the invention lies a reverse list that enables the seamless and automated routing of messages from a specific private interaction address to a public interaction address and then to a second party with whom the first party, which seeks to remain anonymous, communicates.

163. The invention allows users to generate a unique incognito alias that will be used only to facilitate communications with a single second party. The ability to generate a unique incognito alias that can be used only to facilitate communications between a designated second party and a single first party prevents the ability of multiple second parties to cross reference information that might reveal the first party’s identity.

164. The ability to generate a unique incognito alias that can be used only to facilitate communications with a designated second party prevents any other person or business from using that same incognito alias to communicate with the first party – in other words, each

alias is non-transferable. It cannot be handed over or sold to an interloper to allow communication with the first party.

165. The records and reverse lists are stored in non-transitory computer storage to associate addresses in a specific manner, that facilitate their automated routing, management, and specific logic to create, manage, revoke, and synchronize address information in a variety of interactions and pre-interactions.

166. This invention greatly improves the ability of prior art communications systems to facilitate anonymous and easy-to-manage methods of communication.

167. In this way, the '284 patent claims do not simply recite, without more, the mere desired result of anonymously communicating across a communications network in an easy-to-manage method. Rather, the claims recite a specific solution and process for accomplishing that goal.

168. Among the implementations specifically noted was the ability not only to create the relationship between the proxy email but to revoke it.

169. In particular, the specifications indicate that the '284 patent has the potential to allow a third party to mediate a dynamic communication relationship and potentially allow said third-party to leverage the anonymity of the anonymous first-party against the second party.

ii. Blix's Implementation of The '284 Patent

170. The Blix Messaging Bridge, which was launched in 2018 embodies the '284 Patent.

171. Messaging Bridge allows, among other things, third-party app developers to integrate a link in their app that allows users to interact with the app developers anonymously using an incognito email address.

172. App developers are free to integrate this link in multiple end-use scenarios, including to facilitate anonymous sign-in into their apps using an incognito randomly generated email address.

173. Messaging Bridge was developed as a technologically agnostic feature that promotes interoperability by offering seamless integration with all existing email solutions and existing email services. For example, the Blix Messaging Bridge can be deployed as to allow users of an app to communicate anonymously with the app developer using a random incognito email address from their existing, Gmail, Outlook or Apple iCloud Mail mailboxes.

174. The Blix Messaging Bridge functions as a cross-platform proxy, automatically and anonymously relaying private email communications between various email services and applications irrespective of the operating systems on which they run.

175. In addition, the Blix Messaging Bridge allows, among other things, BlueMail users to post an email to social media, such as Twitter, and then engage in secure private messaging with others.

176. Messaging Bridge also allows, among other uses, a business to share an email regarding upcoming discounts on social media, and potential customers could engage in direct communication with the company about that upcoming sale using a manageable *public* interaction address Blix automatically provides—so that the potential customer's incognito email address is never revealed to the business. This feature can be utilized by the users of any email client or email service.

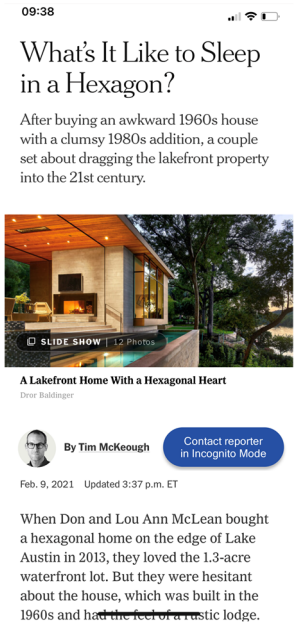
177. The deployment of the Blix Messaging Bridge in apps by third-party app developers to facilitate anonymous incognito user communication is also a potential substantial

source of revenue that the firm could have generated but for Apple's anticompetitive conduct that is described in further detail below.[57]

iii. How Blix Messaging Bridge is Integrated in Third-Party Software

178. Messaging Bridge allows third-party app developers to integrate a link into their app which that allows users to interact with the app developers anonymously using an incognito email address.[58]

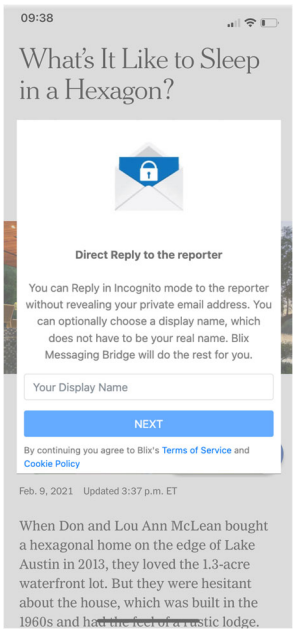
179. An app developer can embed an interaction button in their iOS application which links to the Blix Messaging Bridge and allows users to interact anonymously with the app developer. A screen grab depicting this interaction is attached below:



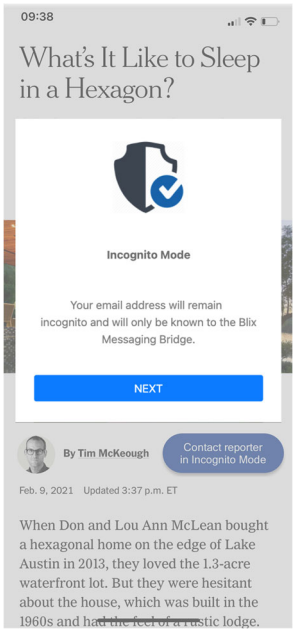
180. Once the user clicks the embedded interaction button, they are directed to the Blix Messaging Bridge and are asked whether they wish to communicate with the app developer using a public alias. A screen grab depicting this interaction is attached below:

[57] *See* Section D(iii)

[58] *See* Section D(ii)

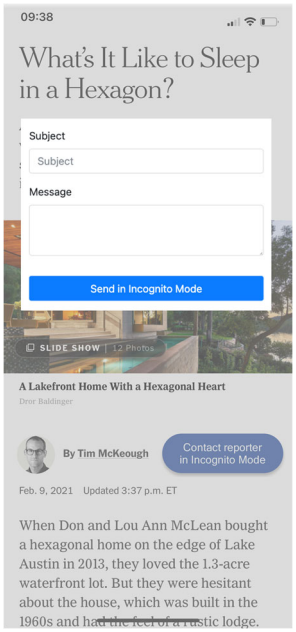


181. The user receives notification that it is now going to be able to communicate anonymously with the app developer via the user's existing email client. A screen grab depicting this interaction is attached below:

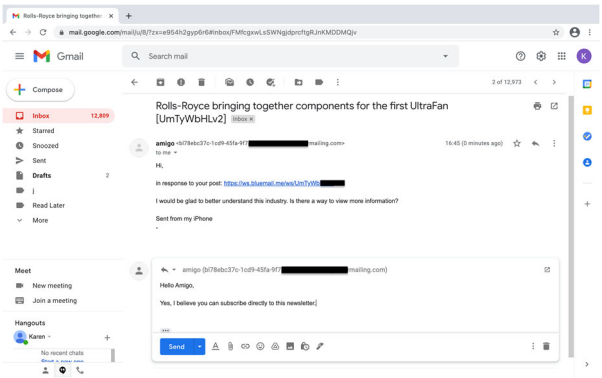


182. Once the verification process is complete, the app's user can use the Blix Messaging Bridge direct messaging widget, which will automatically convert the message to an email and send it to the developer's mailbox. Any subsequent communications can be conducted

either via the user's mailbox as described above or via the Blix Messaging Bridge widget. A screen grab depicting this interaction is attached below:



183. The developer will then receive the incognito email that was relayed via the Blix Messaging Bridge. As the screen grab below shows, the email address or identity of the user that sent the email remains anonymous because the developer receives an incognito email via the Blix Messaging Bridge; only the user's alias is revealed:



184. Crucially, the Blix's embodiment of the invention in the Blix Messaging Bridge is designed to maximize user privacy and interaction control.

185. With respect to user privacy, Blix does not limit the ability of its Messaging Bridge users to communicate anonymously with a pre-designated list of second parties. A Blix user can seamlessly communicate anonymously with their next-door neighbor, the local school board, or an iOS app developer. The ability to seamlessly communicate anonymously with a limitless number of second parties maximizes Blix users' privacy.

186. In addition, as the third party that automatically facilitates the relaying of the users' anonymous communication via the Messaging Bridge, Blix does not utilize data collected or aggregate information about those communications, neither for marketing nor to improve unrelated products or services.

187. With respect to the control exercised by Blix's users, Blix does not revoke or threaten to revoke the ability of its users to communicate anonymously using the Blix Messaging Bridge with any second party unless required by law or for fraud prevention. And even when such revocation is required by law or is necessary to prevent fraud, Blix notifies its users of the expected revocation and then facilitates, if the user so desires, the transfer of the communication between the party to a proxy that in not owned or operated by Blix.

188. Users that rely on the Blix Messaging Bridge are the masters of their relationships with second parties. They can revoke or terminate their communication with a specific second party with ease. Since the user's communication is entirely anonymous, the second party would be unable to continue to communicate with the user, unless that user affirmatively reestablishes that particular line of communication.

189. In addition to maximizing user control over communications, the specific software architecture in the Messaging Bridge decentralizes and limits Blix's own ability to leverage the anonymity of users against a second party with whom they communicate.

190. If Blix must revoke a user's reverse list which facilitates the ability to communicate anonymously, either when required by law or for fraud prevention, Blix will notify that user prior to revocation that such revocation is pending and offer steps to facilitate the continued communication with their contacts outside of Blix's interface.

191. Most importantly, the Blix Messaging Bridge is a cross-platform messaging solution that fosters interoperability and flexibility. It can be deployed on iOS apps, in Twitter links, emails, text messages, and websites. And its automated and secure proxy can relay anonymous incognito emails from one email client or email service to another, whether it be from Outlook to Gmail or from Yahoo to BlueMail. The Messaging Bridge is not limited to a specific OS, nor is it wedded to a specific email client.

iv. Blix's Patent and Products Pose a Substantial Threat to Apple's Monopoly Power in The OS Market, and Apple's Position In the Consumer SSO Market.

192. The '284 Patent and Blix's product philosophy pose a significant threat to Apple's monopoly in the Mobile OS Market.

193. The Blix Messaging Bridge facilitates seamless, anonymous, and user-centric communications which can enable iOS users to privately interact with third-party app developers. This technology can be deployed within third-party apps, creating a secure line of communication between users and developers that is not subject to Apple's control and is insulated from potential surveillance.

194. The ability to generate a unique incognito alias used only to facilitate communications with a single second party also limits Apple's ability to monitor and cross-reference the habits and activity of iOS users across the iOS ecosystem. Apple might be able to track which app an individual user has downloaded or when they are using that app, but it would be unable to surveil the communications between the user and the developer, including any

potential feedback a user may provide regarding that app's performance. This capability is a crucial threat to Apple's ability to closely monitor the success of certain apps and continues its Sherlocking strategy by finding out which "great ideas" are worth "stealing" from app developers.[59]

195. Furthermore, Blix's technology provides a protected pipeline between a developer and user that would allow the developer and user to end-run Apple's strict app-monetization and in-app purchasing guidelines by enabling a private communication channel that can discreetly facilitate app related transactions. For example, while Apple might detect that a third-party developer is processing in-app purchasing using the Blix Messaging Bridge, it would be impossible for Apple to ascertain either transaction volume or revenue garnered using this secure and anonymous payment pipeline.

196. But most notably, the Blix Messaging Bridge can be easily deployed in a Consumer SSO and facilitate seamless, anonymous, and therefore secure user sign-in without the drawbacks of Apple's 'Sign in with Apple' business model, and without the intrusive data-mining characteristic of many Consumer SSOs.[60]

197. This threatening ability, to seamlessly and anonymous log-in and log-out of apps without compromising or monetizing user data, has, upon information and belief, driven Apple to urgently release its own Consumer SSO into the market.

198. Another significant threat is that the Blix Messaging Bridge would securely facilitate what would be otherwise unsafe communications, interactions, and transactions with a new class of developers, entrepreneurs, and service providers. Similar to PayPal in the field of

---

[59] *See* "*Steve Jobs: 'We've Always Been Shameless About Stealing Great Ideas*,'" https://www.huffpost.com/entry/steve-jobs-weve-always-be_n_482791

[60] *See* Section F(ii)

ecommerce transactions, the Blix Messaging Bridge has the potential to facilitate a new class of consumer-developer interactions that have remained untapped due to privacy and security concerns. This technology could facilitate the growth of new online marketplaces that might threaten the way software and services are currently distributed on Mobile OSs.

199. In the context of Mobile OS apps, the Messaging Bridge can render irrelevant many of the "security" and "privacy" oriented curatorial decisions Apple makes when deciding which apps to allow into its walled.

200. The mass adoption of a Consumer SSO solution that hides users' identity throughout all their interactions with app developers has the potential to increase user multihoming—that is, using multiple devices that run different OSs. Consumer SSOs help facilitate a more seamless transition, by disentangling Mobile OS providers from the relationship between end users and app developers. Thus, through its integration into a Consumer SSO solution, the Blix Messaging Bridge would serve as bridge over the moat that Apple has carefully constructed to keep its iOS users locked in, reducing switching costs, facilitating multi-homing, and lessening app developers' dependence on iOS.

201. The increased ease at which users can access a given app in multiple mobile OS using Consumer SSO solutions has the potential to lower the barriers to successfully multihome, which would likely lead some users to exit the Apple iOS system altogether. The Blix Messaging Bridge can enable the reduction in switching costs, facilitate multihoming, and lessen app developers' dependence on iOS and Apple.

202. Existing solutions have been slow to generate meaningful traction because they are incomplete solutions. As explained above, they only hide the users' password in the initial

verification and login process but offer no additional privacy, data, identity protection beyond this basic function.

203. This is supported by a 2020 poll conducted by DataGrail and OnePoll which surveyed 2,000 Americans to understand consumer concern regarding personal data privacy.[61]

204. The poll found that on average, consumers own 27 online accounts, and as people move further online, they expect more control over their personal data.[62]

205. The research showed a growing concern and emphasis on privacy in consumers' relationships with businesses. 80% of Americans think there should be a law in place to protect personal data., and 75% of Americans would boycott their favorite retailer if it failed to keep their personal data safe.[63]

206. In addition, 70% of Americans wish to deny businesses the ability to sell their private data to third parties, and 83% expect to have control over how businesses use their data.[64]

207. Most notably, 68% of Americans expect to be able to *opt-out* of a company selling their private data to a third-party, and 54% of Americans are frustrated by companies that use their personal data to serve targeted personalized ads.[65]

208. The data indicates that at least 68% of American would prefer to use a Consumer SSO that offered complete privacy when interacting with third-party apps if given the opportunity.[66]

---

[61] *See* "*DataGrail's 2020 Consumer Privacy Expectations Report*," https://www.datagrail.io/blog/data-privacy-day-survey/

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.*

209. On information and belief, Apple believes this privacy-focused sentiment is especially prevalent among Apple users and poses problems for Apple regarding adoption of Consumer SSO solutions on iOS. Accordingly, Apple has positioned privacy as core to the consumer value proposition."[67]

210. Apple advertises that its devices and iOS will "protect your privacy and give you control over your information."[68] For example, Apple offers iOS users the ability to control how apps will track their activity.

211. Therefore, iOS users, who are likely more privacy-oriented and less susceptible to trading their data in exchange for free services, would prefer a Consumer SSO solution that effectively guards their personal data.

212. The Blix Messaging Bridge, by facilitating a fully private and anonymous Consumer SSO solution, could potentially address the drawbacks which have slowed the mass adoption of Consumer SSOs by privacy-conscious iOS users. Unlike other Consumer SSOs, which only provide secure login, the integration of the Blix Messaging Bridge would ensures that the user's identity remain incognito in a wide range of interactions with the app developer, such a providing feedback on app performance, making in-app purchases, or engaging in other forms of communication.

213. The embodiment of the '284 patent, the Blix Messaging Bridge has the potential to redefine the way in which end users communicate and interact with third-party developers. Like the introduction of PayPal, which removed barriers of commerce by enabling

---

[67] *See* "Privacy," https://www.apple.com/privacy/#:~:text=Privacy%20is%20a%20fundamental%20human%20right.&text=We%20design%20Apple%20products%20to,you%20control%20over%20your%20information.

[68] *Id.*

users to securely transact with a dazzling array of small and nascent online merchants, the Blix Messaging Bridge has the potential to allow users to securely explore, interact and transact with many smaller and lesser-known app developers and service providers by ensuring that their users data and private information is never disclosed to the provider with which they interact.

214. If Apple becomes firm in the Consumer SSO market, it will not only neutralize the cross-platform threat but will also leverage the technology to keep its users locked into iOS.

215. On the other hand, if a third party like Blix succeeds in marketing and scaling its own solution, it could disintermediate the Consumer SSO experience, lowering the barriers to multi-homing and cross-platform switching, tearing away the walls of Apple's iOS monopoly.

216. The Blix Messaging Bridge allows Blix to offer an anonymous contact service in the Consumer SSO setting. This is not incidental to Blix's plan for the technology. The specification of Blix's '284 patent explicitly recognized that its technology could both create and revoke anonymous communication—the precise function of an SSO solution. And Blix's own use of the '284 patent to expand from anonymous messaging to the implementation Messaging Bridge into Consumer SSOs is a long-planned development which is well-documented.

217. In fact, when this lawsuit was first filed by Blix in October 2019, Ben Volach stated that Apple's exclusionary conduct "hurt…Blix, a successor company launched in September 2019 *to provide corporations with technology outlined in the '284 patent*. As noted in the filing, one of Blix's major features is Messaging Bridge, a system that enables companies to engage with customers through anonymous interactions."[69]

218. Blix is well-positioned to deploy and implement its technology in the context of Consumer SSOs. Blix offers a disruptive business model centered around enterprise solutions,

[69] *See* Exhibit 6 at 2

including integration of the Blix Messaging Bridge into developer and enterprise software. As such, it neither needs to monetize or market data which passes through the Blix Messaging Bridge, nor does it intend to place itself in the middle of the communicative relationship to lock in users and firms. Instead, as a privacy- and consumer-centric company, it would simply offer the Blix Messaging Bridge service to its core enterprise customers to allow their users to sign-in and communicate anonymously with developers across multiple platforms and OS ecosystems, reducing barriers to switching and encouraging multi-homing.

219. Blix's implementation of the '284 patent technology in the Blix Messaging Bridge fosters disintermediation: A business and a customer who both use Blix's anonymous communication system can continue their commercial relationship without fearing that Blix will exploit its involvement as a proxy to harvest their data or leverage its position as an intermediary to exploit the second party.

E. Apple's Anticompetitive Conduct to Neutralize Blix and the Emergence of Competitive Privacy-Driven Messaging Technology

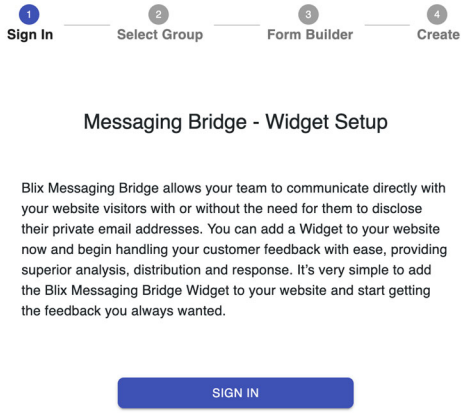
i. Apple Put Sand in Blix's Gears and Sabotaged its Plans to Scale its Technology in Order to Maintain its Monopoly Power in the Mobile OS Market

220. The application for the '284 patent was first published on April 21, 2016, more than a year before the patent was duly and legally issued.

221. On information and belief, Apple became aware of the '284 Patent prior to August 2018.

222. In 2018, Blix introduced the '284 patent technology via the Blix Messaging Bridge. The "Share Email" feature powered by the Blix Messaging Bridge facilitates anonymous communications and prevents dissemination of email addresses to uninvited senders. On information and belief, from 2018 onwards, Apple gained a better understanding and the ability

to scrutinize the technology and in particular to learn how the Blix Messaging Bridge functioned. A screen grab of the Blix Messaging Bridge widget configuration is shown below:



223. On information and belief, either prior to the events described above, Apple took overt steps to sabotage the ability of Blix to scale its innovative Messaging Bridge technology.

224. From May 21, 2019 and until June 3, 2019 engaged in a series of pretextual act to sabotage Blix's ability to market the Blix Messaging Bridge.[70] The mentioned conduct, which is described in great detail in Blix's First Amended Complaint, has harmed Blix and delayed to scale the deployment and sale of its Blix Messaging Bridge solution to companies, including third-party app developers.

225. And, although this conduct did not foreclose Blix's ability to market BlueMail, Apple successfully shifted Blix's focus and limited recourses during this critical time from marketing and further implementing Messaging Bridge in other use cases to constantly fighting Apple's persistent bullying.

[70] *See* Exhibit 9

ii. Apple's Infringement of the '284 Patent

226. On June 3, 2019, the motivation behind Apple's destructive conduct and acts toward Blix became apparent. Apple announced it had been developing its own version of the Blix Messaging Bridge; its baseless anticompetitive harassment of Blix was a deliberate effort to delay Blix's ability to scale in iOS while Apple was building and finalizing its own infringing product.

227. On June 3, 2019, Apple announced its new 'Sign In With Apple' service. Apple's Senior Vice President of Software Engineering Craig Federighi unveiled the service. Mr. Federighi explained that Apple, like many software developers, recognized the growing need for a Consumer SSO that protected user privacy; "personal information" too often "gets shared" through online communication, something Apple "wanted to solve" through its new 'Sign In With Apple' service.[71]

228. Mr. Federighi described the 'Sign In With Apple' service as "the fast, easy way to sign in without all of the tracking."[72] This system used a new application programming interface (API) that would permit users to log in to and communicate with applications in a new and more private manner: "you are authenticated with Face ID on your device, logged in with a new account without revealing any new personal information." Users would be able to log in, but "Keep your email private."[73] As Mr. Federighi explained, the new system worked by assigning public-facing random addresses for the application to interact with the user. These interaction addresses were intended to be easily manageable, relaying communications from public

[71] *See* Exhibit 9

[72] *Id.*

[73] *Id.*

interaction addresses to private interaction addresses using "a unique random address that forwards to your real address."[74]

229. Mr. Federighi further explained that this private relay system would assign multiple interaction addresses to facilitate a user's ability to manage interactions with applications; each user would receive a separate interaction address for interactions with specific developers: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great."[75]

230. Mr. Federighi further explained that Apple was offering this system for manageable communications to protect the privacy of users, and to respond to growing demand among users: Giving third parties your electronic addresses information "can be convenient, but it also can come at the cost of your privacy. Your personal information sometimes gets shared behind the scenes and these logins can be used to track you. We wanted to solve this and many developers do too." But the solution was not Apple's to use—it was the same system Mr. Volach had already patented several years earlier.[76]

231. In other presentations at Apple's Worldwide Developer Conference in June 2019, Apple continued to feature 'Sign In With Apple' to encourage software developers to use infringing features of the 'Sign In With Apple' service in their software applications. For example, after the keynote address, three Apple engineers gave a separate presentation entitled "Introducing Sign In With Apple."[77]

---

[74] *Id*

[75] *Id*

[76] *Id.*

[77] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/706/. An excerpt from Apple's transcript of that presentation, taken from the same website, is attached. *See* D.I. 13-5, Exhibit 5 to Amended Complaint.

232. During this hour-long presentation, Apple's engineers gave a large crowd of software developers detailed instructions on how to use the infringing functionality of 'Sign In With Apple.' Those engineers explained that users would often create a host of false, hard-to-manage public interaction addresses to protect their privacy: Apple touted its "Private Relay" service as the solution to this problem, noting that the 'Sign In With Apple' system would automatically create email addresses shared between the end-user and the application developer.

233. A developer's emails to this public address would be automatically forwarded to the user's private address, such that the user could receive email while hiding its email address from the application developer and thereby, prevent harvesting of this information: Apple touted the "Hide My Email" and "Private Relay" system as a significant step forward in protecting user's privacy, while still enabling easy-to-manage electronic communication.

234. Apple encouraged software developers to use the new API that Apple would be releasing for Apple devices (such as iPhones and iPads running iOS 13), claiming that the API offered a solution for users who desire privacy because its "Hide My Email" features would enable a private "Two-way relay" for "Any email communication" between parties: In another presentation entitled "Designing for Privacy," Apple engineers instructed developers to use infringing features of 'Sign In With Apple' in their applications in order to more effectively reach customers concerned with privacy: "we think this is your best shot at getting your emails in front of your customers."[78]

235. Apple engineers acknowledged that "People can be hesitant to share their real email address" because of privacy problems created by sharing interaction addresses; "We've all

[78] A video of this presentation is available online at https://developer.apple.com/videos/play/wwdc2019/708/. An excerpt from Apple's transcript of that presentation, taken from the same website, is attached. *See* D.I. 13-6, Exhibit 6 to Amended Complaint.

seen email lists stolen or resold and then abused by spammers." Apple employees described Apple's new private relay service and 'Sign In With Apple' as the best way to facilitate interaction without sharing private interaction addresses:

> Customers can choose to hide their email address, in which case you'll get an address managed by Apple through which we relay your emails to the customer and vice versa....
>
> For each customer, this managed address is different for each developer, so customers are in control of which developers they want to receive email from, and you're in control of who can send emails to the managed address we provide you, since you can whitelist domains or addresses that we'll accept incoming mail from.

236. This presentation by Apple engineers further explained that the code in Apple's new API for 'Sign In With Apple' was configured specifically to enable trusted interactions, allowing a software developer to know they are communicating with the intended user even without knowing the user's private interaction address: "With Sign In With Apple, we can leverage on-device intelligence to provide you with one bit that indicates a user is likely real. And that flag is supported on iOS, and we provide it at account creation."

237. Apple's website offers further instructions to developers and end-users on how to utilize infringing aspects of the 'Sign In With Apple' service.

238. For example, Apple tells developers that 'Sign In With Apple' was built from the ground up to give users peace of mind about their privacy," because it offers a secure and private platform for anonymous messaging: "Apple's private email relay lets users receive email even if they prefer to keep their address private."[79] Apple likewise tells end-users the ability to use the infringing features of 'Sign In With Apple.' For example: "Sign in with Apple is the fast,

[79] *See* "Overview: Sign In With Apple," https://developer.apple.com/sign-in-with-apple/.

easy, and more private way to sign into apps and websites using the Apple ID that you already have."[80]

239. Apple further instructs developers to use Apple's "Private Email Relay Service" to meet users' growing demand for a private and secure communication system that protects their privacy. Apple tells third-party software developers that "Some privacy-conscious users will choose to keep their personal email address private and use Apple's private email relay service when setting up an account. To send email messages through the relay service to the users' personal inboxes, you will need to register your outbound email domains."[81] Apple likewise instructs end-users to use the infringing features of 'Sign In With Apple': "You can use Hide My Email—Apple's private email relay service—to create and share a unique, random email address that forwards to your personal email. That way you can receive useful messages from the app without sharing your personal email address. Only the registered app or site developer can communicate with you using this email, and you can turn it off at any time."[82]

240. Apple's detailed instructions to software developers instruct them to register up to 10 interaction addresses to use for communications with 'Sign In With Apple' users. Specifically, Apple instructs developers: "In order to send email messages through the relay service to the users' personal inboxes, you will need to register your outbound email domains," that "registered domains must create Sender Policy Framework (SPF) DNS TXT records in order to transit Apple's private mail relay," and that a developer "can register up to 10 domains and communication emails" to communicate with 'Sign In With Apple' users through the "Private

[80] *See* "What is Sign in with Apple?" *https://support.apple.com/en-us/HT210318*

[81] *See* "Make Signing in Easy," https://developer.apple.com/sign-in-with-apple/get-started/.

[82] *See* "How to use Sign in with Apple," https://www.digitaltrends.com/mobile/how-to-use-sign-in-with-apple/

Email Relay Service."[83] Apple likewise gives detailed instructions to end-users on how to use infringing features for anonymous communication[84] and for interaction address management.[85]

241. Apple's 'Sign In With Apple' system clearly infringes Mr. Volach's patented techniques in the '284 patent. Yet Apple never sought permission to use these techniques, never acknowledged that these techniques originated with Mr. Volach, and never offered to pay for using his patented technology.

242. Apple's introduction of 'Sign In With Apple' had an immediate adverse effect, buttressing Apple's walled iOS garden and expanding its monopoly power by actively and deliberately harming iOS users and third-party developers.[86]

iii. Apple's Tie in the Consumer SSO Market

243. An additional blow landed in August 2019, when Apple announced that developers would have to implement 'Sign In With Apple' in their apps.

244. In particular, Apple's 'App Store Review Guidelines' stated that "Apps that use a third-party login service must also offer 'Sign in with Apple' as an equivalent option."

245. This decision significantly restricted Blix's ability to market or offer the Blix Messaging Bridge to app developers.

246. On June 7, the App Store Review Guidelines also stated that developers must "Prominently display a Sign In with Apple button. Make a Sign In with Apple button the same size or larger than other sign-in buttons and avoid making peoples scroll to see the button."[87]

---

[83] *See* D.I. 13-9, Exhibit 9 to Amended Complaint

[84] *See* "Hide My Email for Sign in with Apple," https://support.apple.com/en-us/HT210425#hideemail.

[85] *See* "Manage the apps you use with Sign in with Apple," https://support.apple.com/en-us/HT210426.

[86] *See* Section F(ii)

[87] *See* "Human Interfaces Guidelines," https://urldefense.proofpoint.com/v2/url?u=https-3A__developer.apple.com_design_human-2Dinterface-2Dguidelines_sign-2Din-2Dwith-

247. On June 7, the App Store Review Guidelines further stated that developers must "Position a Sign In with Apple button correctly in relation to other sign-in buttons. In a stacked layout, place the Sign In with Apple button above the other buttons."[88]

248. These two provisions were subsequently removed from the App Store Review Guidelines.

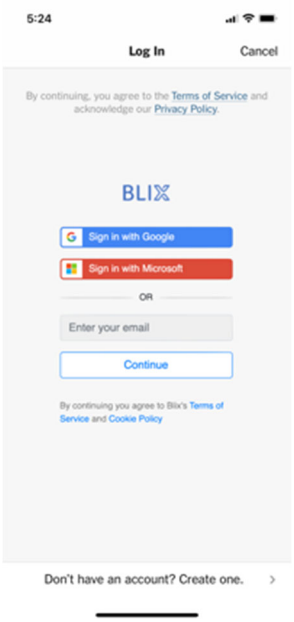
249. Apple is free to offer its competing Consumer SSO solution, as long as that product does not infringe on the intellectual property of Blix. But Apple did not intend to compete on the merits, but it contractual tie and exclusionary restrictions impede, entrants, but most notability Blix to compete for developer adoption.

250. In order to deploy the Messaging Bridge within an app and allow the app's user to communicate with the developer anonymously using incognito mode, including upon initial set up and sign in, Blix has to verify and link the user's 'private' email address with Messaging Bridge. This due to the fact that Messaging Bridge is centered on email communication, and therefore needs users to enter their email service when setting they decide to use Messaging Bridge.

251. Blix offers users the option to verify their email using 'Sign in with Google' or 'Sign in with Microsoft' to allow for this seamless linkage. A screen grab depicting this interaction is attached below:

2Dapple_overview_&d=DwIFAg&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=Ux2y5hMtOWTn7Bz3_FSe_NK0vh_FuHz3jjvGbgbXuEo&m=KRQ9P23afoIubxRKxx961LTcT-Z3ILHDLNUBDwfx-wY&s=kBdeWkFGUzRhaAbA9lnloGi4bHhWTmN6kY8P7M9Kt-w&e=

[88] *Id.*



252. After Apple announced that "Apps that use a third-party or social login service (such as Facebook Login, Google Sign-In, Sign in with Twitter, Sign In with LinkedIn, Login with Amazon, or WeChat Login) to set up or authenticate the user's primary account with the app must also offer 'Sign in with Apple' as an equivalent option,"[89] Blix was forced to pick its poison.

253. On the one hand, if Blix kept the ability to authenticate the user's identity and email address by implementing 'Sign in with Google' or 'Sign in with Microsoft', it would also be required, per Apple's 'App Store Review Guidelines,' to also offer their users 'Sign in with Apple.' This would render the deployment of the Blix Messaging Bridge within a third-party app obsolete.

254. 'Sign in with Apple' incorporates the 'Hide My Email' feature. Therefore, once a user decides to authenticate their user's identity and email address via 'Sign in with

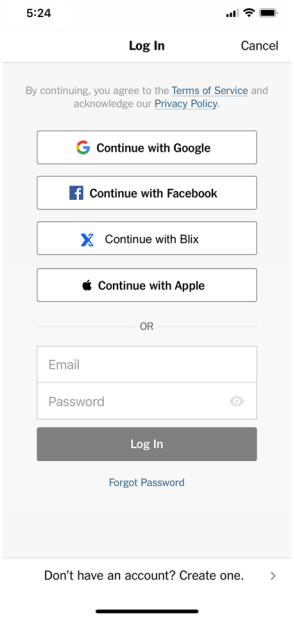
[89] *See* "App Store Review Guidelines," Section 4.8, https://developer.apple.com/app-store/review/guidelines/#sign-in-with-apple

Apple' Apple also asks the user whether they wish to provide the app developer with a tokenized email address.

255. Accordingly, if a user chooses to authenticate their identity and email address via 'Sign in with Apple' they already engaged in the process of hiding their true address.

256. So why would that user then decide to go through the extra steps of using the Blix Messaging Bridge to generate another incognito email address if they already generated an equivalent one when they authenticated their identity with 'Sign in with Apple'?

257. To sum, in this scenario, which is depicted in the screen mock-up depicted attached below, the Blix Messaging Bridge will be rendered duplicative and obsolete:



258. On the other hand, if Blix could choose to remove the ability of users to authenticate their identity and email address by removing the option of using 'Sign in with Google' or 'Sign in with Microsoft' in order to avoid Apple's tie, this removal would present a serious loss of core functionality. The user could no longer use the Blix Messaging Bridge as part of a mail client to centralize communications across email boxes. Blix's application would no longer be a seamless and convenient communication solution for user-developer

communications. By requiring Blix to incorporate Apple's tied product, Apple gave itself an advantage over Blix's Messaging Bridge, even within Blix's own product. The Blix Messaging Bridge would be immediately rendered as a less seamless and convenient solution to communicate while remaining anonymous with an app developer in comparison to Apple's bundled solution that allows for seamless verification *and* private communication.

259. Apple's tie foreclosed Blix's ability to scale its Messaging Bridge feature and compete with the same company that stole its invention: Apple.

260. Apple's 'Sign In With Apple' is not new software functionality that was integrated by Apple into iOS. Rather, Apple contractually ties third-party developer access to iOS and the App Store to a mandate requiring them to offer 'Sign In With Apple' when they offer their users access to their app using a third-party or social login service. In particular, non-compliance with Apple's App Store Review Guidelines, including the 'Sign In With Apple' mandate, would result in rejection from the App Store.

261. Apple's contractual tie of 'Sign In With Apple' does not improve the value of iOS to users or to third-party app developers.

iv. Apple Continues to Target and Harm Blix

262. On the same day that Apple announced the launch of 'Sign In With Apple,' June 3, 2019, Apple continued to sabotage Blix's ability to market products incorporating the Blix Messaging Bridge. Apple's conduct throughout June is detailed in the First Amended Complaint.[90]

263. Apple's conduct up to this point in time can be summed up as an effort to sabotage and delay the ability of Blix's technology to generate traction in the iOS ecosystem.

[90] *See* Exhibit 9

This was achieved by limiting consumer exposure to the Blix Messaging Bridge which was deployed on BlueMail and by preventing the ability of potential Blix customers, including Apple developers, to implement the Blix Messaging Bridge in their own iOS apps. In addition, Apple's conduct forced the company to shift its focus and limited resources from scaling, deploying, marketing and further improving the technology to dealing with Apple's constant and deliberate anticompetitive harassment and obstructionist behavior.

264. In December 2019, after six months of constant anticompetitive harassment, Apple finally contacted Blix to discuss the suppression of products that embodied the Blix Messaging Bridge and agreed to stop the suppression, albeit temporarily.[91] Upon information and belief, Apple's conduct throughout this period was aimed at putting sand in Blix's gears by forcing the company to shift focus and limited resources from scaling , deploying, marketing, and further improving the technology to dealing with Apple's constant and deliberate anticompetitive harassment and obstructionist behavior.

265. On August 14, 2019, Apple's anticompetitive harassment of Blix continued. Apple rejected Blix's request to change the company's name on iOS from BlueMail to Blix. Apple provided no explanation for its refusal. Upon information and belief, Apple's decision to refuse to update Blix's name on iOS was motivated by a desire to blur the lines between BlueMail and the Blix Messaging Bridge. Apple's decision significantly limited Blix's ability to market and promote the Blix Messaging Bridge as a stand-alone feature on Mobile OS that could be deployed beyond its original use-case within BlueMail and in conjunction with third-party apps like Twitter and websites. Only four days before this Second Amended Complaint was due

[91] *See* Exhibit 9

to be filed, Apple suddenly and without any explanation decided to approve Blix's request – a year and half after the request was first submitted.

266. In parallel, Blix decided to sue Apple for the above-referenced conduct and on October 4, 2019, filed the first Complaint in this case.[92]

267. On February 12, 2020, Engadget published an article that covered the story surrounding BlueMail's return to the App Store. The story contained a statement from Blix and a comment from an Apple spokesperson. In particular, the spokesperson claimed that BlueMail was not approved because it "had technical issues."[93] The spokesperson added that "Blix is proposing to override basic data security protections which can expose users' computers to malware that can harm their Macs and threaten their privacy."[94]

268. On March 9, 2020, Blix's counsel pointed out to Apple that it made false assertions and demanded that Apple immediately cease further false and defamatory statements.

269. On August 13, 2020 Apple ratcheted up its efforts to put sand in Blix's gears by directly blocking the ability of Blix to push updates on iOS because, according to Apple, BlueMail did not support 'Sign In With Apple,' and therefore was in violation Guideline 4.8 – Sign in with Apple." In particular Apple stated that apps "that use a third-party login service for account authentication must offer 'Sign in with Apple' to users as an equivalent option" and instructed Blix to "revise your app to offer 'Sign in with Apple' as an equivalent login option."

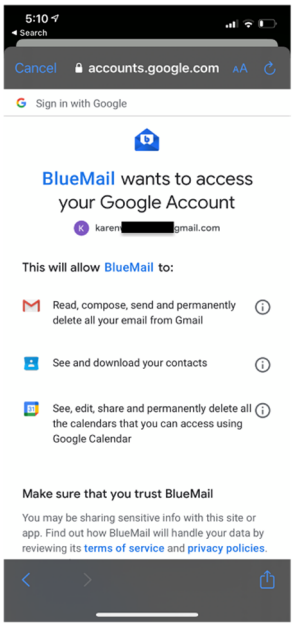
270. Blix pointed out to Apple that BlueMail does not offer a third-party login service. In particular, that Guideline 4.8 applied only to instances where Consumer SSOs were

[92] *See* D.I. 1

[93] *See* "BlueMail is back in the App Store after it called out Apple (update)," https://www.engadget.com/2020-02-12-bluemail-back-in-the-apple-app-store.html

[94] *Id.*

offered as a login option. In contrast, Blix integrated Consumer SSOs in its BlueMail app to allow its users that were already logged in to import their contacts and data from their existing mailboxes, including Gmail and Outlook. A screen grab depicting this scenario is attached below:



271. On information and belief, Apple's decision to block the ability of Blix to push updates on iOS under Guideline 4.8 was pretextual. At all relevant times Apple knew that BlueMail was not required to offer its users the option of using 'Sign in with Apple,' knew that BlueMail did not violate Guideline 4.8, and did not in good faith believe BlueMail was subject to Guideline 4.8. Apple's vague rejection was part of Apple's scheme to limit Blix's ability to scale its Blix Messaging Bridge feature although they knew all too well that BlueMail was an email client.

272. On August 15, 2020, Apple doubled down on its decision to block the ability of Blix to push updates on iOS, yet again citing "Guideline 4.8 – Sign in with Apple" and baselessly argued that Blix did not comply with this provision.

273. On September 15, 2020 Apple refused to allow Blix to implement necessary updates in its BlueMail app, yet again citing "Guideline 4.8 – Sign in with Apple" and arguing that Blix did not comply with this provision.

274. On September 16, 2020, Apple announced that it would allow other email clients to be set as the default apps for email communications on iOS. But Apple, without any justification, delayed Blix's ability to become the default mail app until October 5, 2020.

275. On September 29, 2020, Business Insider published an article that covered the story surrounding Apple's decision to reject all app updates that Blix was trying to push on iOS "in part because of BlueMail's lack of a "Sign in with Apple" feature."[95] It revealed that Apple finally allowed Blix to push updated to iOS on September 28, 2020 after Business Insider reached out to Apple to solicit an explanation for Apple's conduct. As Blix did not make any changes in the binary or metadata on the App Store, Apple's decision was not the result of any change made by Blix but directly as a result of public pressure for accountability.

276. Finally, on October 2, 2020, Apple filed a petition for Inter Partes Review of the '284 patent before the Patent Trial and Appeal Board seeking to invalidate the '284 patent that is embodied in Blix's disruptive and innovative Messaging Bridge.[96]

F. Harm To Competition

i. Apple's Anticompetitive Embrace and Extend Strategy

277. As mentioned, Apple's illegal effort was directed at squashing the competitive threat posed by Blix's communication technology and the Blix Messaging Bridge in order to

[95] *See* "An email app developer that's been at odds with Apple says the iPhone maker stonewalled its app update for weeks," https://www.businessinsider.com/apple-blix-bluemail-app-store-update-sign-in-with-apple-2020-9

[96] *See* Exhibit 8

maintain its monopoly in Mobile OS. Apple's anti-competitive conduct took the form of an "embrace and extend" strategy.

278. First, Apple "embraced" Blix's technology by copying it from Blix and thereby infringing the '284 Patent. While Apple was in the process of developing its own features that embody the '284 Patent it also ensured that Blix would not be able to scale its own original version of the technology by constantly sabotaging Blix's own deployment efforts.

279. Second, Apple "extended" Blix's technology by forcing third-party app developers that incorporated Consumer SSO solutions in their apps to also offer Apple's own 'improved' and 'privacy focused' Consumer SSO solution, 'Sign In With Apple' through a contractual tie arrangement and exclusionary terms.

280. Apple coerced third-party iOS app developers into a tie-in and exclusionary arrangement in which they had to implement Apple's 'Sign In With Apple' in their apps. In particular, Apple used its distribution channels including the App Store and app development guidelines, to flood the market with its corrupted and inferior version of Blix's technology in an attempt to hijack Blix's technology and transform it into one of Apple's proprietary and hallmark features.

281. Apple also embedded strategic, anticompetitive features into 'Sign In With Apple' and the development tools products.[97]

282. Apple's strategic, anticompetitive features that were implemented into 'Sign In With Apple' and were designed to entrench and exercise its market power in the Mobile OS market to impose harmful economic and technical constraints on app developers and iOS users.

[97] *See* Section F(ii)

ii. 'Sign In With Apple' Uses the Pretext of User Privacy as an Anticompetitive Weapon Against Developers

283. Apple argues that 'Sign In With Apple' is a far superior solution in comparison to existing offerings because it does not compromise user data and ensures that the identity of an app's end users remains hidden.

284. In reality, 'Sign In With Apple' unnecessarily injects Apple as a gatekeeper that possesses the ability to oversee and control the relationship between third party developers and its end users. 'Sign In With Apple' could have achieved Apple's stated privacy goals by less restricting means. Most notably, the Blix Messaging Bridge is a less restrictive alternative.

285. First, Apple does not offer iOS users the ability to 'hide' their email outside of 'Sign In With Apple.' For instance, an iOS user cannot 'hide' their email address through Apple's mail app. This means that iOS users who choose to 'hide' their email cannot also communicate anonymously with their next-door neighbors, the neighborhood school board or even service providers or business entities. They can only communicate anonymously with app developers.

286. When 'Sign In With Apple' was first introduced, Apple's own engineers stated that people "can be hesitant to share their real email address" because of privacy problems created by sharing interaction addresses, further explaining that "We've all seen email lists stolen or resold and then abused by spammers."[98]

287. But surprisingly, since the 'hide my email' feature is only available within 'Sign In With Apple,' this feature does not address the problem Apple's own engineers have

[98] *See* "Designing for Privacy," https://developer.apple.com/videos/play/wwdc2019/708

identified, namely, the ability of parties to steal email lists or of spammers to flood the mailboxes of iOS users.

288. If Apple truly sought to address the problem that its own engineers 'identified', it would have also incorporated the 'hide my email' feature in the Apple mail app, thereby allowing iOS users to communicate anonymously with their next-door neighbors, the neighborhood school board or even service providers or business entities.

289. Second, when a user first downloads an app and decides to sign-in with 'Sign In With Apple', they are prompted with the 'hide my email' toggle button before the user even makes any attempt to communicate with the app developer. On information and belief, the only reason for including this prong is so Apple can generate a reverse list, as that list is described in the '284 patent, that includes the tokenized emails of all of the users that decided to use 'Sign In With Apple' and link them to the address the developer provided Apple for the purpose of implementing 'Sign In With Apple'.

290. In essence, Apple uses the 'hide my email' toggle to generate a reverse list for each individual app that includes the tokenized addresses of all the users that used 'Sign In With Apple' to sign-in. As the '284 patent explains, a third-party intermediary that facilitates communications between first-party iOS users and a second party app developer can easily revoke the reverse list it generated and cut all communication lines between the apps' users and the developers.

291. The ability to revoke the reverse list gives Apple immense power over developers as the sole mediator between app developers and a segment of their users. This leverage over developers further solidifies its monopoly power in the mobile OS market by further locking developers into its ecosystem.

292. Many, or even all, of an iOS user's relationships with streaming providers, retailers, gaming networks, and other firms can be potentially mediated through 'Sign In With Apple.' If a user uses 'Sign In With Apple' to access a third-party app, Apple does not provide the user with an alternative username or alternative address with which to sign into their account. If users decide to leave the Apple ecosystem, they lose the ability to access their accounts if Apple decides to revoke the reverse list. At a minimum, it would take multiple steps of contact with the third-party developer to re-establish the relationship. This could be especially damaging if the users engaged in multiple in-app purchases or has made significant progress in a gaming app. The process promises to be more stressful than canceling one's credit card and restoring multiple payment relationships because the end-user will be nearly untraceable on the other side.

293. For app developers, the intermediation and threat of revocation is even more serious. Assume, hypothetically, a business has one-third or one-half of its user base on iOS connected through 'Sign In With Apple', and the company breaks with Apple over some business disagreement. If Apple revokes its propriety reverse list, that business loses all ability to communicate individually with those stranded users.

294. The app developer does not have the email addresses of its users and it cannot log-in into 'Sign In With Apple' to retrieve even the users' tokenized email addresses. The users may try to reconnect with the developer, but it would be virtually impossible for the developer to match their true identity to the tokenized addresses Apple generated for them. Take the example of gamers, who both build characters or profiles, and spend money on in-app purchases. If the developer lost contact with a large number of players, some portion of the player population could be expected to reach out and reclaim their accounts. But with hundreds or thousands of hours invested, and tens or hundreds of dollars, in these gaming creations, some players might

use the confusion to attempt to hijack a valuable account belonging to someone else. Without an accurate reverse list to authenticate the players, the developer has no way to ensure the authenticity of players' claims to accounts.

295. Such an event would be disastrous and catastrophic for a developer's business and could be compared to a fire breaking out in a bank and consuming all of the bank's deposit records.

296. A potent demonstration of this immense power was recently on display. Last year, as part of ongoing dispute between software developer Epic and Apple, Apple threatened to revoke Epic's ability to access or use 'Sign In With Apple.' Fearing the threat of permanently losing a substantial portion of its user base due to the inability of those users to log in and access their Epic accounts, Epic desperately tried to contact its iOS users and ask them to provide Epic with a public email address so they could reestablish their user accounts after Apple pulled the switch.[99]

297. For reasons that are not completely clear, Apple did not follow up on its threat, but the way in which Apple leveraged the threat of revoking the reverse list that it generates through 'Sign In With Apple' demonstrates how the company can force developers to remain in Apple's good graces.[100]

298. Leah Culver, the cofounder and chief technology officer of podcast discovery app Breaker, commented in general that she's "not super happy about [Apple] forcing apps to use a certain type of login, and I think it's kind of petty." She added: "The question becomes,

---

[99] *See* "Apple's in a war for the future of the App Store. Here's what's at stake," https://www.cnn.com/2020/09/25/tech/apple-fortnite-epic-games-lawsuit/index.html

[100] *See* "Epic says 'Sign In with Apple' will keep working for Fortnite after all," https://www.theverge.com/2020/9/10/21431396/epic-sign-in-with-apple-will-keep-working-fortnite

just because they control the App Store, should they control the login?" Culver says. She also noted that Google doesn't force Android developers to use Login with Google, something Google confirmed.[101]

299. Apple's use of its dominant market power in mobile OS to flood the market with its Consumer SSO solution, 'Sign In With Apple', ensured that developers would have to comply with Apple's demands and rules or risk losing a sizable portion of their userbase.

300. But more importantly, Apple's ability to continuously flood the market with its Consumer SSO solution, 'Sign In With Apple' via the contractual tie means that with every day that passes, more and more of an app's iOS users use 'Sign In With Apple', and an ever greater portion of that app's iOS users base becomes a hostage of Apple.

301. This is not the first time that Apple used Privacy as pretext justifying anticompetitive behavior, as discussed in the anticompetitive conduct section above. However, this perhaps the most insidious and egregious iteration.

302. As demonstrated above, Apple's implementation of the 'Hide my Email' feature in 'Sign In With Apple' is another clear example of Apple using privacy as a sword to exclude rivals and shield to insulate itself from liability for maintaining its monopoly power in the Mobile OS market. In doing so, Apple not only harms third-party app developers and rivals or potential entrants in the Mobile OS market but holds their own iOS users as hostages, or bargaining chips, mere instrumentalities in Apple's unquenchable thirst for monopoly power.

[101] *See* "App Makers Are Mixed on 'Sign In With Apple,'" https://www.wired.com/story/sign-in-with-apple-mixed-reactions/

iii. Apple's Decision to Flood The Market With Its Corrupted and Inferior Version of Blix's Technology Harms Third-Party Developers and Users

303. In addition, Apple's 'extend' strategy, which involved contractually tying 'Sign In With Apple' to third-party developers' ability to distribute apps on iOS, effectively prevents Blix from deploying the technology it created to compete with 'Sign In With Apple' in the Consumer SSO market.

304. Apple's ability to foreclose nascent competition in the Consumer SSO market through its illegal tying arrangement harms third-party app developers, iOS users, and competitors in or potential entrants to the Mobile OS market. All of these stakeholders are deprived of a superior Consumer SSO solution developed by Blix using its '284 Patent.

305. Apple only incorporates its 'Hide My Email' feature only within 'Sign In With Apple'. This means that users who wish to communicate anonymously with second parties other than app developers cannot do so. In contrast, Blix allows users to communicate privately and anonymously, not only with third-party app developers, but any second party they choose.

306. By limiting the use of the copycat 'hide my email' feature to its Consumer SSO and its walled garden of curated and vetted third-party apps, Apple ensures that the most destabilizing capabilities of the '284 patent are underutilized by its Mobile OS users.

307. This decision by Apple stifles innovation and deprives users of numerous, potentially groundbreaking apps.

308. Apple champions 'Sign In With Apple' as a product "built from the ground up to give users peace of mind about their privacy." But in reality, Apple's own terms and

conditions state that "Apple may use information [collected through 'Sign In With Apple'] that does not identify you to improve Apple products and services" and "for marketing."[102]

309. Apple's claim that privacy to justifies its tying arrangement is a pretext. Apple supposedly implemented the 'hide my email' feature in 'Sign In With Apple' to limit privacy abuse by third parties, including "abuse[] by spammers." But Apple's own Privacy Policy allows it to collect data from iOS users that choose to 'hide' their email and use that data for marketing purposes.

310. In other words, Apple does not want its iOS users to be "abused by [third party] spammers" but will make an exception as long as the spam is generated and circulated by Apple itself.

311. In contrast, Blix's Terms and Conditions and Privacy Policy state that the Blix Messaging Bridge does not utilize data or aggregate information about the relaying of its users' private communications for marketing purposes or to improve unrelated products or services.[103]

312. Further, Apple allows developers to integrate "Sign In With Google" as long as it is not used for authentication. This is inconsistent with the privacy rationale—if its users feared giving their data to Google, implementing a Google sign-in to an iOS native app in any way would pose the same issue.

313. In contrast to Blix, Apple sees these private communications as its own, and threatens to revoke the ability of its users to communicate with developers or even login into

[102] *See* "Apple Card & Privacy," https://support.apple.com/en-us/HT210699#:~:text=Apple%20may%20use%20information%20that,with%20Apple%20data%20we%20receive.

[103] *See* Exhibit 7

their user account if a developer decides to leave the iOS ecosystem or if Apple feels that an app developer has fallen out of line, an incredibly powerful tool to enforce compliance.

314. Blix has utilized specific software architecture in the Blix Messaging Bridge to maximize user control over their communications and deployed its invention in a manner that decentralizes and limits Blix's own ability to leverage the anonymity of its users against the second party with whom they communicate.

315. In particular, Blix generates a reverse list for each of its individual users and the reverse list is then updated every time the user actually wishes to interact with an additional second party. The reverse list generated by Blix for each user contains all the users' tokenized aliases which are used to communicated with second parties and the addresses of those second parties communication is relayed. Thus, if Blix has to revoke a user's reverse list, either when required by law and for fraud prevention, this act of revocation only affects a single individual user and its ability to continue to communicate anonymously with second parties.

316. In contrast Apple's reverse lists are based on individual apps as opposed to individual iOS users. The reasoning behind this design decision is simple, it makes it much easier to terminate the ability of any given app developer to continue to communicate with their customers, iOS users be damned.

317. Thus, Apple's decision to infringe the '284 patent, to put sand in Blix's gears and to tie its own adulterated implementation of Blix's technology prevents the ability of Blix to offer its own SSO solution and thereby deprives iOS users and third-party app developers from access to a far superior potential SSO solution.

318. Apple's motivation in engaging in this anticompetitive behavior is primarily motivated from its desire to maintain its monopoly power in the Mobile OS market by embracing

and extending an adulterated version of a technological innovation that it perceived as threatening its hegemony.

VI. COUNT I

A. Infringement of the '284 Patent

319. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

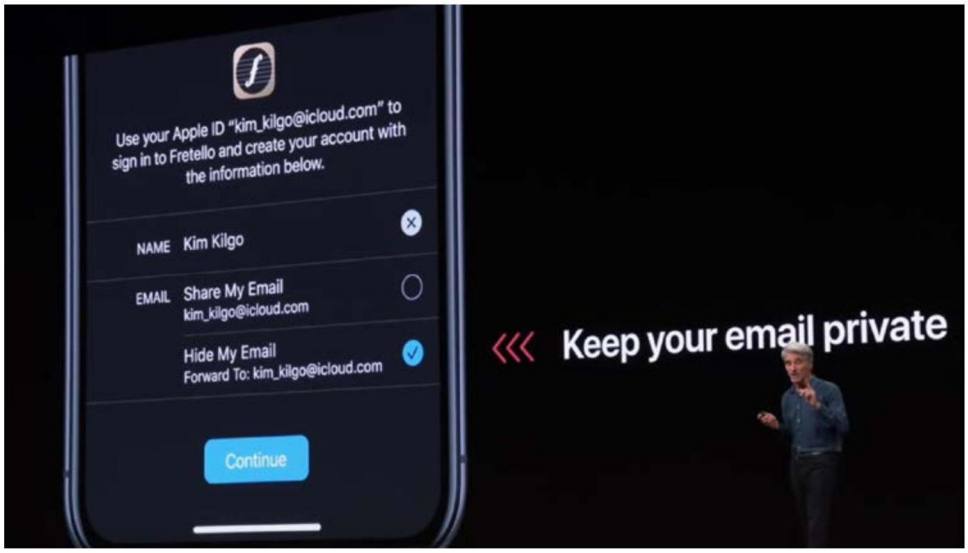
320. As explained herein, and on information and belief, Apple has directly infringed, and continues to directly infringe, at least claims 1-5, 7-10, 13, 18, 21-22, 28-30, 33-34, and 36-37 of the '284 patent by making, using, offering for sale, selling, and/or importing into the United States the infringing 'Sign In With Apple' system, including iOS devices with an API specifically configured to perform infringing operations, and has contributed to and/or induced infringement of the '284 patent by others, including software developers and end-users.

321. For example, and without limitation, on information and belief the 'Sign In With Apple' system meets every limitation of at least claim 1 of the '284 patent, and Apple's making, using, offering for sale, selling, and/or importing the 'Sign In With Apple' system, including iOS devices running iOS 13, and Apple's distribution of iOS 13 to such devices, directly infringes claim 1 of the '284 patent under 35 U.S.C. § 271(a).

322. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, perform a method of controlled pre-interaction between a first party and at least one second party. For example, a first party, such as an end-user of an Apple device, and at least one second party, such as an application developer, can perform controlled pre-interaction, such as operations performed prior to communications between the end-user and the application developer, to ensure that subsequent communications via private relay will not inform the application developer of the end user's private email address. It claims

"Apple's private email relay lets users receive email even if they prefer to keep their address private."[104] Moreover, 'Sign In With Apple' will also perform controlled pre-interaction operations for at least login and authentication purposes; when using the 'Sign In With Apple' system, "you are authenticated with Face ID on your device, logged in with a new account without revealing any new personal information." [105]

323. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, provides at least one private interaction address of said first party. For example, Apple presents to a first party, such as an end-user of an Apple device, at least one private interaction address of that end-user, such as an email address. Apple provides this email address to users upon sign-in via an interface asking users if they wish to "Share My Email" or "Hide My Email," as shown below:



See also D.I. 13-4, Exhibit 4 to Amended Complaint

[104] *See* D.I. 13-7, Exhibit 7 to Amended Complaint

[105] *See* D.I. 13-4, Exhibit 4 to Amended Complaint

324. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, defines at least one manageable public interaction address for said first party. For example, Apple defines a random email address for an end-user who selects the "Hide My Email" option. [106] This email address is designed to be manageable and can be disabled at any time by an end-user: "we give each app a unique random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great." [107]

325. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, forms a record, wherein said manageable public interaction address is associated with said private interaction address for said first party. For example, when the random email address receives an email from a specific application developer, Apple forwards that email to the end-user's private email address. On information and belief, Apple forwards these messages using records that associate the random email address with the user's private email address.

326. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, generates a reverse list, wherein an interaction address of said second party is associated at least with said manageable public interaction address of said first party. For example, the interaction address of an application developer is associated with an end-user's random address when the "Hide My Email" option is selected. Apple associates each random email address with one specific application developer: "we give each app a unique

[106] *See* D.I. 13-4 and 13-5, Exhibits 4 and 5 to Amended Complaint

[107] *See* D.I. 13-4, Exhibit 4 to Amended Complaint

random address. This means you can disable any one of them at any time when you are tired of hearing from that app. It's really great." [108]

327. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, performs at least one pre-interaction act, said pre-interaction act comprises accessing said reverse list, and identifying said interaction address of said second party in said reverse list. For example, on information and belief, Apple accesses a reverse list to identify the email address of an application developer before forwarding email to that application developer via its private relay service.

328. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, determines that said manageable public interaction address of said first party is associated, at said reverse list, with said interaction address of said second party. For example, on information and belief, the 'Sign In With Apple' private relay system determines that a randomly generated email address associated with an end-user is also associated with an application developer, at least in order to ensure that communications to the randomly generated email address are only forwarded to the end-user if they are received from the application developer.

329. The 'Sign In With Apple' system, including Apple devices specifically configured to work with that system, performs a method wherein said interaction address of said second party is obtainable from a third party or external services provider, wherein at least one reverse list entry is formed by synchronizing said interaction address of said second party with said manageable public interaction address. For example, on information and belief, Apple's 'Sign In With Apple' service allows application developers to register email addresses that are

[108] *See* D.I. 13-4, Exhibit 4 to Amended Complaint

obtainable from third parties and external services providers, including obtainable from Apple. Moreover, on information and belief, at least one reverse list entry in Apple's 'Sign In With Apple' system is formed by synchronizing an application developer's registered email address with the randomly assigned email address assigned for an end-user's communications with that application developer.

330. Apple's own use of Apple devices specifically configured to use the 'Sign In With Apple' system and set that system in motion, including without limitation use during testing of devices such as iPhones and iPads running iOS 13, directly infringes at least claim 1. These infringing uses include, without limitation, Apple's testing in the United States of said devices, as well as Apple's demonstrations of the infringing method, including demonstrations to application developers, media, end-users, and to potential customers—including, on information and belief, demonstrations by Apple Store employees at the Apple Store in this District.

331. Apple's making, using, offering for sale, selling, and/or importing devices specifically configured to use the 'Sign In With Apple' system and set that system in motion, including without limitation devices (such as iPhones and iPads) running iOS 13, infringes at least claims 28-30 and 33-37.

332. Thus, the use of Apple's 'Sign In With Apple' system meets every limitation of at least claim 1. Moreover, the sale of iOS devices specifically configured to use and place that system in motion infringe at least claims 28-30 and 33-37. Apple directly infringes at least those claims by offering the 'Sign In With Apple' system, and devices specifically configured to place that system in motion, in violation of 35 U.S.C. § 271(a).

333. Apple has also indirectly infringed, and continues to indirectly infringe, the claims of the '284 patent by inducing infringement pursuant to 35 U.S.C. § 271(b) and/or contributing to infringement pursuant to 35 U.S.C. § 271(c).

334. On information and belief, in violation of 35 U.S.C. § 271(b), Apple specifically intended to induce infringement of the '284 patent by application developers and end-users of Apple devices and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that their inducing acts would cause infringement.

335. On information and belief, Apple knew of the '284 patent since at least as early as June 2019, when Apple removed the competing BlueMail product from the App Store only days after announcing its infringing 'Sign In With Apple' system. Apple has also known of the '284 patent, and of its infringement of that patent, at least since filing and service of the original Complaint.

336. On information and belief, Apple's customers directly infringe the '284 patent. For example, when an end-user uses the 'Sign In With Apple' system in the manner intended by Apple, including for the purposes of communicating via private relay between an end-user and an application developer by way of a randomly assigned unique email address, those activities infringe at least claim 1 of the '284 patent. Similarly, when Apple software developers use the 'Sign In With Apple' system in this manner for reciprocal communications with end-users, those activities likewise infringe at least claim 1 of the '284 patent.

337. On information and belief, Apple specifically intends for end-users and application developers to directly infringe the '284 patent. Apple encourages infringement by instructing end-users and application developers by way of product support, developer

documentation, and live instructional presentations that instruct users and applications developers on how to use the infringing 'Sign In With Apple' system.

338. On information and belief, despite Apple's knowledge of the '284 patent and knowledge that end-users and application developers will necessarily infringe the '284 patent when using the 'Sign In With Apple' system as instructed, Apple continues to encourage infringement.

339. Apple's 'Sign In With Apple' application programming interface (API) is specifically designed to perform the infringing functionality described herein. This API has no substantial non-infringing uses; it is designed to carry out the infringing functionality that forms the basis for Plaintiff's patent infringement claims.

340. Defendant also contributes to infringement of the '284 patent by Apple's end-users and application developers in violation of 35 U.S.C. §271(c). On information and belief, Apple knew of the '284 patent since at least as early as June 2019, when it chose to eliminate an embodiment of that patent from the App Store only days after announcing its competing and infringing 'Sign In With Apple' system. On information and belief, Apple offers to sell and sells within the United States devices specifically configured to operate with the 'Sign In With Apple' system knowing that they constitute a material part of the claimed inventions, knowing that the 'Sign In With Apple' API is especially made or especially adapted for use in infringing the '284 patent, and knowing that the 'Sign In With Apple' system is not a staple article or commodity of commerce suitable for substantial non-infringing use.

341. Apple has committed and continues to commit all of the above acts of infringement without license or authorization.

342. As a result of Apple's infringement of the '284 patent, Plaintiff has suffered damages and will continue to suffer damages.

343. On information and belief, Apple's infringement of the '284 patent has been and continues to be willful. Apple has had knowledge of BlueMail and, on information and belief, has had knowledge of the '284 patent, since Apple decide to remove the BlueMail embodiment from the App Store days after announcing its competing and infringing 'Sign In With Apple' service. On information and belief, Apple copied the '284 patent's innovative disclosures, including features used in the BlueMail software, before excluding the BlueMail software application from the Apple App Store. Apple offered a competing system for private communication knowing the risk of infringement and/or in view of a risk of infringement that was sufficiently obvious that it should have been known to Apple. Despite this risk, Apple has deliberately continued to infringe in a wanton, malicious, and egregious manner, with reckless disregard for Plaintiff's patent rights. Defendant's infringing actions have been and continue to be consciously wrongful, entitling Plaintiff to increased damages under 35 U.S.C. § 284.

344. Under 35 U.S.C. § 283, Plaintiff is entitled to injunctive relief precluding further infringement. Apple's wrongful conduct has caused and will continue to cause Plaintiff to suffer irreparable harm resulting from the loss of its lawful patent right to exclude others from making, using, selling, offering to sell, and/or importing Plaintiff's patented inventions. On information and belief, Apple will continue to infringe the '284 patent unless enjoined by this Court.

VII. COUNT II

A. Monopolization Under 15 U.S.C. § 2 –Monopoly Maintenance

345. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

346. Apple has monopoly power in the United States with respect to Mobile OS. Apple has a 61.47% or greater market share in Mobile OS by unit of phones. Apple's market share by revenue, on information and belief, exceeds this figure. There are barriers to entry, including high cost and network effect, that preclude entry of new competitors.

347. Apple has the ability to and does exclude competition in the form the aftermarket for distribution of iOS apps. This exclusion is direct evidence of its monopoly power.

348. There are no reasonably interchangeable substitutes for Mobile OS. Only Mobile OS can run mobile devices, and mobile devices must have a Mobile OS to run.

349. There are no reasonably interchangeable substitutes for the iOS App Store. This is the only way Apple permits users to put apps onto a device running iOS, and the only way that developers can get their apps onto users' devices. Technical workarounds are so prohibitively difficult and disfavored that they remain a *de minimus* fringe.

350. Apple has willfully maintained its monopoly power through its course of anticompetitive conduct, including through artificially raising the transaction cost to its user base of leaving the Apple ecosystem. Apple's (a) infringement of the '284 patent technology; (b) requirement that app developers selling in the iOS App Store offer 'Sign In With Apple'; and (c) implementation of 'Sign In With Apple' in a manner that allows Apple to terminate communications between developers and end users, are exclusionary and anticompetitive. Through its course of conduct, Apple has excluded competition and willfully maintained its monopoly in Mobile OS through means other than competing on the merits.

351. In so doing, injury to Plaintiff was both a necessary and intended effect. In maintaining its iOS monopoly and extending its hold over users and developers for iOS, Apple

has infringed Blix's '284 patent, excluded its BlueMail application prevented it from deploying its embodiment of the '284 patent, the Blix Messaging Bridge on iOS, and prevented Blix's entry into the market for Consumer SSOs. Apple has thereby inflicted substantial antitrust injury on Plaintiff in violation of the Sherman Act, § 2.

352. Through its conduct, Apple has succeeded in acquiring and maintaining a monopoly in the relevant markets, has used and continues to use that monopoly to impose a supracompetitive tax that raises prices both to developers and end users of iOS. In addition, Apple is using and will continue to use its monopoly power in the relevant markets to artificially thwart competition from cross-platform interoperable services that lower switching costs, reduce user demand for Apple's iOS, and threaten Apple's supracompetitive prices for its devices and for distribution on the iOS App Store. Increasing the transaction costs of an end user's switch from Apple's iOS locks the end users in and extends and maintains its Mobile OS monopoly in which Apple can charge a monopoly rent for sales of and through apps to these users.

353. Apple's conduct has had a substantial effect on interstate and foreign commerce. As alleged herein, Apple's conduct has involved trade or commerce in the United States which has a direct, substantial, and reasonably foreseeable effect, and which gives rise to Blix's claim, on trade or commerce in the United States, including Blix's efforts to engage in such trade or commerce in the United States.

354. Blix has suffered and will suffer irreparable injury of the type that the antitrust laws were intended to prevent. As explained herein, Apple's actions substantially harm competition, discouraging entry by software developers and limiting choice for consumers. Among other things, its conduct has excluded competition by Blix (and by other developers' applications), reduced consumer choice among applications, reduced developer incentives to

invest in entering the relevant markets and developing innovative applications, raised significant barriers to entry, raised rival's costs to compete, tilted the playing field in Apple's favor, made it harder for Blix and other developers to compete, artificially set and increased prices and decreased output for applications, reduced competition over protecting user privacy, and artificially increased demand for Apple's devices and platforms (including by excluding competition from cross-platform interoperable services that lower switching costs, reduce user demand for Apple's iOS, and threaten Apple's supracompetitive prices for its devices).

355. Blix has been and will be irreparably injured by the harm to competition resulting from Apple's conduct.

356. Blix has been and will be irreparably injured in its business or property as a result of Apple's conduct.

357. There is no procompetitive justification for Apple's exclusionary conduct in maintaining its Mobile OS monopoly.

358. Apple willfully maintains its monopoly power over the Mobile OS market through its anticompetitive conduct described above. In so doing, Apple inflicted substantial antitrust injury on Plaintiff in violation of § 2 of the Sherman Act and is liable to Plaintiff for damages in an amount to be determined at trial.

VIII. COUNT III

A. Monopoly Tying Under 15 U.S.C. §§ 1 and 2

359. The allegations in the preceding paragraphs are incorporated by reference as if fully set forth herein.

360. For purposes of this claim, the relevant product tying market is the Mobile OS market. The relevant tied market is the Consumer SSO market. The relevant geographic market is the United States.

361. In the Mobile OS market, Apple has 61.47% or more of the market by units, and a greater percentage by revenue. It has a monopoly in this market. Through the use of its market power in the tied market, Apple can force developers to take and implement products in a separate market.

362. By the use of its market power in the Mobile OS market, Apple requires developers to take, and to implement with their applications software, 'Sign In With Apple' if they take and implement any other Consumer SSO. Apple makes the acceptance of 'Sign In With Apple' a condition of developing for iOS, and of offering their products through the iOS App Store. Apple requires all developers who have already chosen to implement a different Consumer SSO to now, at the developer's cost, also implement 'Sign In With Apple.' Apple also requires any developer that decides in the future to choose to implement a different Consumer SSO, to also at its cost implement 'Sign In With Apple.' Because Apple's developer base for iOS is so large, Apple's requirement that developers take 'Sign In With Apple' has affected a substantial volume of commerce.

363. Mobile OS and Consumer SSO are different markets.

364. Offerings in the Mobile OS market and the Consumer SSO market are separate products.

365. The adoption of 'Sign In With Apple,' Apple's Consumer SSO service, is the product of actual contractual coercion. Apple unilaterally changed its developer agreement to require that any developer doing business with Apple in the Mobile OS market, also accept 'Sign In With Apple' if it used any Consumer SSO for user verification purposes. This includes developers who had already chosen to implement a Consumer SSO from another source.

366. It is not in developers' interest to offer 'Sign In With Apple.' Apple can, and in one instance has, used the threat of revoking access to 'Sign In With Apple' and potentially deprive a developer of any contact with its own customers as a tool of control when the developer raises a dispute with Apple. Some developers have in the past, and still prefer to, do business with different Consumer SSO providers, but may not do so under Apple's Developer Guidelines, which developers cannot contest, because of Apple's market power in the tying market and aftermarket.

367. Through this tying requirement, Apple has harmed competition in a substantial amount of interstate commerce. Apple's tying arrangement has: (a) blocked Plaintiff, a nascent competitor with a disruptive business model, from including its Messaging Bridge with any product, and from offering any product in the Consumer SSO market; (b) required developers to implement 'Sign In With Apple' at their own cost, even if they had already chosen or wanted to choose to implement a Consumer SSO from another source; and (3) reduced innovation and increased the cost to consumers of Apple's Consumer SSO, 'Sign In With Apple' by allowing Apple to mediate and terminate their relationships with third party service providers at will, thereby incurring significant consumer harm.

IX. JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully demands a trial by jury of all issues so triable.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that judgment be entered in favor of Plaintiff and against Apple as follows:

A. A judgment that the '284 Patent is directly and indirectly infringed by Apple's offers to sell, sales of, and uses of the 'Sign In With Apple' system within the

United States, or importation into the United States of products, including without limitation iOS products and other products using the 'Sign In With Apple' API, that practice one or more of the inventions claimed in the '284 Patent;

B. A judgment that Apple's conduct, as alleged, is unlawful under § 2 of the Sherman Act;

C. An order preliminary and permanently enjoining Apple, its affiliates and subsidiaries, and each of its officers, agents, and employees and those acting in privity or concert with them, from making, using, offering to sell, selling, importing products or systems claimed in any of the claims of the '284 Patent, and from causing or encouraging others to use, sell, offer for sale, or import products or systems that infringe any claim of the '284 Patent, until after the expiration date of the '284 Patent, including any extensions and/or additional periods of exclusivity to which Plaintiff is or may become entitled;

D. A permanent injunction prohibiting Apple from further illegal monopolization of the Mobile OS and Consumer SSO Markets;

E. An order that Apple violated § 1 of the Sherman Act;

F. An order preliminary and permanently enjoining Apple, its affiliates and subsidiaries, and each of its officers, agents, and employees and those acting in privity or concert with them, from continuing the practice of tying third-party app developers ability to distribute applications in iOS to the implementation of Apple's 'Sign In With Apple' Consumer SSO in said applications.

G. An award of damages under 35 U.S.C. § 284 in an amount sufficient to compensate Plaintiff for its damages arising from Apple's infringement,

including, but not limited to, lost profits and/or a reasonable royalty, together with pre-judgment and post-judgment interest, and costs;

H. An award of damages adequate to compensate Blix for Apple's illegal conduct, based on lost sales, lost profits, price erosion, loss of market share, or any other theory the Court finds applicable, together with pre-judgment and post-judgment interest;

I. An order awarding treble damages for willful infringement by Apple, pursuant to 35 U.S.C. 284;

J. An order awarding treble damages under 15 U.S.C. § 15;

K. An accounting and/or supplemental damages for all damages occurring after any discovery cutoff and through the Court's decision regarding the imposition of a permanent injunction;

L. A judgment declaring that this case is exceptional and awarding Plaintiff its reasonable costs and attorneys' fees pursuant to 35 U.S.C. § 285;

M. An award to Plaintiff of its reasonable attorney's fees and costs under 15 U.S.C. § 15; and

N. Such other relief as this Court or a jury may deem proper and just under the circumstances.

ASHBY & GEDDES

/s/ Andrew C. Mayo

John G. Day (#2403)
Andrew C. Mayo (#5207)
500 Delaware Avenue, 8th Floor
P.O. Box 1150
Wilmington, DE 19899
(302) 654-1888
jday@ashbygeddes.com
amayo@ashbygeddes.com

Attorneys for Plaintiff

Of Counsel:

Daniel J. Melman
Guy Yonay
Sarah Benowich
Shaoul Sussman
PEARL COHEN ZEDEK LATZER BARATZ LLP
Times Square Tower
7 Times Square, 19th Floor
New York, NY 10036
(646) 878-0800

Mark C. Rifkin
Thomas H. Burt
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
270 Madison Avenue, 9th Floor
New York, NY 10016
(212) 545-4600

Dated: February 12, 2021